WatchGuard®
Firebox® X Edge
User Guide

Firebox X Edge - Firmware Version 7.1

WatchGuard®

Certifications and Notices

FCC Certification

This appliance has been tested and found to comply with limits for a Class A digital appliance, pursuant to Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This appliance may not cause harmful interference.

- This appliance must accept any interference received, including interference that may cause undesired operation.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Notice

The CE symbol on your WatchGuard Technologies equipment indicates that it is in compliance with the Electromagnetic Compatibility (EMC) directive and the Low Voltage Directive (LVD) of the European Union (EU).

ϵ

Industry Canada

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe A respecte toutes les exigences du Reglement sur le materiel broulleur du Canada.

CANADA RSS–210

The term "IC:" before the radio certification number only signifies that Industry of Canada technical specifications were met.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

VCCI Notice Class A ITE

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス A 情報技術装置です。この装置を家庭用環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Declaration of Conformity

DECLARATION OF CONFORMITY

WatchGuard Technologies, Inc.
505 Fifth Ave. S., Suite 500
Seattle, WA 98104-3892
USA

WatchGuard Technologies Inc. hereby declares that the product(s) listed below conform to the European Union directives and standards identified in this declaration.

Product (s):
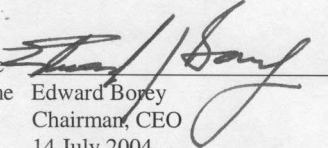
Internet Firewall with VPN, Models MF16S32E10, MF4S16E5

EU Directive(s):

Low Voltage (73/23/EEC)
Electromagnetic Compatibility (89/336/EEC)

Standard(s):

EN60950 3rd Ed. (1999) Safety of ITE

EN50022 (1998), Class A   Emissions for ITE
EN50024 (1998)   Immunity for ITE

Signature
Full Name   Edward Borey
Position   Chairman, CEO
Date   14 July 2004

Notice to Users

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

WatchGuard Firebox Software
End-User License Agreement

IMPORTANT - READ CAREFULLY BEFORE ACCESSING WATCHGUARD SOFTWARE:

This Firebox Software End-User License Agreement ("AGREEMENT") is a legal agreement between you (either an individual or a single entity) and WatchGuard Technologies, Inc. ("WATCHGUARD") for the WATCHGUARD Firebox software product, which includes computer software components (whether installed separately on a computer workstation or on the WATCHGUARD hardware product or included on the WATCHGUARD hardware product) and may include associated media, printed materials, and on-line or electronic documentation, and any updates or modifications thereto, including those received through the WatchGuard LiveSecurity Service (or its equivalent), (the "SOFTWARE PRODUCT"). WATCHGUARD is willing to license the SOFTWARE PRODUCT to you only on the condition that you accept all of the terms contained in this Agreement. Please read this Agreement carefully. By installing or using the SOFTWARE PRODUCT you agree to be bound by the terms of this Agreement. If you do not agree to the terms of this AGREEMENT, WATCHGUARD will not license the SOFTWARE PRODUCT to you, and you will not have any rights in the SOFTWARE PRODUCT. In that case, promptly return the SOFTWARE PRODUCT, along with proof of payment, to the authorized dealer from whom you obtained the SOFTWARE PRODUCT for a full refund of the price you paid. The WATCHGUARD hardware product is subject to a separate agreement and limited hardware warranty included with the WATCHGUARD hardware product packaging and/or in the associated user documentation.

1. Ownership and License. The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. This is a license agreement and NOT an agreement for sale. All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and applets incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by WATCHGUARD or its licensors. Your rights to use the SOFTWARE PRODUCT are as specified in this AGREEMENT, and WATCHGUARD retains all rights not expressly granted to you in this AGREEMENT. Nothing in this AGREEMENT constitutes a waiver of our rights under U.S. copyright law or any other law or treaty.

2. Permitted Uses. You are granted the following rights to the SOFTWARE PRODUCT:

(A)   You may install and use the SOFTWARE PRODUCT on any single WATCHGUARD hardware product at any single location and may install and use the SOFTWARE PRODUCT on multiple workstation computers.

(B)   To use the SOFTWARE PRODUCT on more than one WATCHGUARD hardware product at once, you must purchase an additional copy of the SOFTWARE PRODUCT for each additional WATCHGUARD hardware product on which you want to use it. To the extent that you install copies of the SOFTWARE PRODUCT on additional WATCHGUARD hardware products in accordance with the prior sentence without installing the additional copies of the SOFTWARE PRODUCT included with such WATCHGUARD hardware products, you agree that use of any software provided with or included on the additional WATCHGUARD hardware products that does not require installation will be subject to the terms and conditions of this AGREEMENT. You must also maintain a current subscription to the WatchGuard LiveSecurity Service (or its equivalent) for each additional WATCHGUARD hardware product on which you will use a copy of an updated or modified version of the SOFTWARE PRODUCT received through the WatchGuard LiveSecurity Service (or its equivalent).

(C)	In addition to the copies described in Section 2(A), you may make a single copy of the SOFTWARE PRODUCT for backup or archival purposes only.

3. Prohibited Uses. You may not, without express written permission from WATCHGUARD:

(A)	Use, copy, modify, merge or transfer copies of the SOFTWARE PRODUCT or printed materials except as provided in this AGREEMENT;

(B)	Use any backup or archival copy of the SOFTWARE PRODUCT (or allow someone else to use such a copy) for any purpose other than to replace the original copy in the event it is destroyed or becomes defective;

(C)	Sublicense, lend, lease or rent the SOFTWARE PRODUCT;

(D) Transfer this license to another party unless

(i) the transfer is permanent,

(ii) the third party recipient agrees to the terms of this AGREEMENT, and

(iii) you do not retain any copies of the SOFTWARE PRODUCT; or

 (E) Reverse engineer, disassemble or decompile the SOFTWARE PRODUCT.

4. Limited Warranty. WATCHGUARD makes the following limited warranties for a period of ninety (90) days from the date you obtained the SOFTWARE PRODUCT from WATCHGUARD or an authorized dealer:

(A) Media. The disks and documentation will be free from defects in materials and workmanship under normal use. If the disks or documentation fail to conform to this warranty, you may, as your sole and exclusive remedy, obtain a replacement free of charge if you return the defective disk or documentation to WATCHGUARD with a dated proof of purchase.

(B) SOFTWARE PRODUCT. The SOFTWARE PRODUCT will materially conform to the documentation that accompanies it. If the SOFTWARE PRODUCT fails to operate in accordance with this warranty, you may, as your sole and exclusive remedy, return all of the SOFTWARE PRODUCT and the documentation to the authorized dealer from whom you obtained it, along with a dated proof of purchase, specifying the problems, and they will provide you with a new version of the SOFTWARE PRODUCT or a full refund, at their election.

Disclaimer and Release. THE WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD, AND YOUR REMEDIES, SET FORTH IN PARAGRAPHS 4, 4(A) AND 4(B) ABOVE ARE EXCLUSIVE AND IN SUBSTITUTION FOR, AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD AND ITS LICENSORS AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD AND ITS LICENSORS, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN THE SOFTWARE PRODUCT (INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, ANY WARRANTY OF NONINFRINGEMENT, ANY WARRANTY THAT THE SOFTWARE PRODUCT WILL MEET YOUR REQUIREMENTS, ANY WARRANTY OF UNINTERRUPTED OR ERROR-FREE OPERATION, ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE (WHETHER ACTIVE, PASSIVE OR IMPUTED) OR FAULT OF WATCHGUARD AND ITS LICENSORS AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE TO, OR CAUSED BY OR CONTRIBUTED TO BY, THE SOFTWARE PRODUCT).

Limitation of Liability. WATCHGUARD'S LIABILITY (WHETHER IN CONTRACT, TORT, OR OTHERWISE; AND NOTWITHSTANDING ANY FAULT, NEGLIGENCE, STRICT LIABILITY OR PRODUCT LIABILITY) WITH REGARD TO THE SOFTWARE PRODUCT WILL IN NO EVENT EXCEED THE PURCHASE PRICE PAID BY YOU FOR SUCH PRODUCT. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY. IN NO EVENT WILL WATCHGUARD BE LIABLE TO YOU OR ANY THIRD PARTY, WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT), FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF OR IN CONNECTION WITH THIS WARRANTY OR THE USE OF OR

INABILITY TO USE THE SOFTWARE PRODUCT, EVEN IF WATCHGUARD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY.

5. United States Government Restricted Rights. The SOFTWARE PRODUCT is provided with Restricted Rights. Use, duplication or disclosure by the U.S. Government or any agency or instrumentality thereof is subject to restrictions as set forth in subdivision (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, or in subdivision (c)(1) and (2) of the Commercial Computer Software -- Restricted Rights Clause at 48 C.F.R. 52.227-19, as applicable. Manufacturer is WatchGuard Technologies, Inc., 505 5th Ave. South, Suite 500, Seattle, WA 98104.

6. Export Controls. You agree not to directly or indirectly transfer the SOFTWARE PRODUCT or documentation to any country to which such transfer would be prohibited by the U.S. Export Administration Act and the regulations issued thereunder.

7. Termination. This license and your right to use the SOFTWARE PRODUCT will automatically terminate if you fail to comply with any provisions of this AGREEMENT, destroy all copies of the SOFTWARE PRODUCT in your possession, or voluntarily return the SOFTWARE PRODUCT to WATCHGUARD. Upon termination you will destroy all copies of the SOFTWARE PRODUCT and documentation remaining in your control or possession.

8. Miscellaneous Provisions. This AGREEMENT will be governed by and construed in accordance with the substantive laws of Washington excluding the 1980 United National Convention on Contracts for the International Sale of Goods, as amended. This is the entire AGREEMENT between us relating to the SOFTWARE PRODUCT, and supersedes any prior purchase order, communications, advertising or representations concerning the SOFTWARE PRODUCT AND BY USING THE SOFTWARE PRODUCT YOU AGREE TO THESE TERMS. IF THE SOFTWARE PRODUCT IS BEING USED BY AN ENTITY, THE INDIVIDUAL INDICATING AGREEMENT TO THESE TERMS REPRESENTS AND WARRANTS THAT (A) SUCH INDIVIDUAL IS DULY AUTHORIZED TO ACCEPT THIS AGREEMENT ON BEHALF OF THE ENTITY AND TO BIND THE ENTITY TO THE TERMS OF THIS AGREEMENT; (B) THE ENTITY HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THIS AGREEMENT AND PERFORM ITS OBLIGATIONS UNDER THIS AGREEMENT AND; (C) THIS AGREEMENT AND THE PERFORMANCE OF THE ENTITY'S OBLIGATIONS UNDER THIS AGREEMENT DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH THE ENTITY IS A PARTY. No change or modification of this AGREEMENT will be valid unless it is in writing and is signed by WATCHGUARD.

Version: 040226

Copyright, Trademark, and Patent Information

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

The mod_ssl package falls under the Open-Source Software label because it's distributed under a BSD-style license. The detailed license information follows.

Copyright (c) 1998-2003 Ralf S. Engelschall. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/)."

4. The names "mod_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.

5. Products derived from this software may not be called "mod_ssl" nor may "mod_ssl" appear in their names without prior written permission of Ralf S. Engelschall.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY

THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1. This software is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

2. The origin of this software must not be misrepresented, either by explicit claim or by omission. In practice, this means that if you use PCRE in software that you distribute to others, commercially or otherwise, you must put a sentence like this:

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England.

somewhere reasonably visible in your documentation and in any relevant files or online help data or similar. A reference to the ftp site for the source, that is, to:

ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/

should also be given in the documentation. However, this condition is not intended to apply to whole chains of software. If package A includes
PCRE, it must acknowledge it, but if package B is software that includes
package A, the condition is not imposed on package B (unless it uses
PCRE independently).

3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. If PCRE is embedded in any software that is released under the GNU General Purpose License (GPL), or Lesser General Purpose License (LGPL), then the terms of that license shall supersede any condition above with which it is incompatible.

The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

PLEASE NOTE: Some components of the WatchGuard WFS software incorporate source code covered under the GNU Lesser General Public License (LGPL). To obtain the source code covered under the LGPL, please contact WatchGuard Technical Support at:

877.232.3531 in the United States and Canada
+1.360.482.1083 from all other countries

This source code is free to download. There is a $35 charge to ship the CD.

This product includes software covered by the LGPL.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it

too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of

it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

 "Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves,

then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during

execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system rather than copying library functions into the executable, and (2) operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to

these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

PLEASE NOTE: Some components of the WatchGuard WFS software incorporate source code covered under the GNU General Public License (GPL). To obtain the source code covered under the GPL, please contact WatchGuard Technical Support at:

877.232.3531 in the United States and Canada
+1.360.482.1083 from all other countries

This source code is free to download. There is a $35 charge to ship the CD.

This product includes software covered by the GPL.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our

decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Limited Hardware Warranty

This Limited Hardware Warranty (the "Warranty") applies to the enclosed Firebox hardware product, not including any associated software which is licensed pursuant to a separate end-user license agreement and warranty (the "Product"). BY USING THE PRODUCT, YOU (either an individual or a single entity) AGREE TO THE TERMS HEREOF. If you do not agree to these terms, please return this package, along with proof of purchase, to the authorized dealer from which you purchased it for a full refund. WatchGuard Technologies, Inc. ("WatchGuard") and you agree as set forth below or on the reverse side of this card, as applicable:

1. LIMITED WARRANTY. WatchGuard warrants that upon delivery and for one (1) year thereafter (the "Warranty Period"): (a) the Product will be free from material defects in materials and workmanship, and (b) the Product, when properly installed and used for its intended purpose and in its intended operating environment, will perform substantially in accordance with WatchGuard applicable specifications.

This warranty does not apply to any Product that has been: (i) altered, repaired or modified by any party other than WatchGuard except for the replacement or inclusion of specified components authorized in and performed in strict accordance with documentation provided by WatchGuard; or (ii) damaged or destroyed by accidents, power spikes or similar events or by any intentional, reckless or negligent acts or omissions of any party. You may have additional warranties with respect to the Product from the manufacturers of Product components. However, you agree not to look to WatchGuard for, and hereby release WatchGuard from any liability for, performance of, enforcement of, or damages or other relief on account of, any such warranties or any breach thereof.

2. REMEDIES. If any Product does not comply with the WatchGuard warranties set forth in Section 1 above, WatchGuard will, following receipt of the product you claim is defective and at its option, either (a) repair the Product, or (b) replace the Product; provided, that you will be responsible for returning the Product and for all costs of shipping and handling. Repair or replacement of the Product shall not extend the Warranty Period. Any Product, component, part or other item replaced by WatchGuard becomes the property of WatchGuard. WatchGuard shall not be responsible for return of or damage to any software, firmware, information or data contained in, stored on, or integrated with any returned Products.

3. DISCLAIMER AND RELEASE. THE WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD, AND YOUR REMEDIES, SET FORTH IN PARAGRAPHS 1 AND 2 ABOVE ARE EXCLUSIVE AND IN SUBSTITION FOR,

AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN THE PRODUCT (INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, ANY WARRANTY OF NONINFRINGEMENT, ANY WARRANTY OF UNINTERRUPTED OR ERROR-FREE OPERATION, ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE (WHETHER ACTIVE, PASSIVE OR IMPUTED) OR FAULT OF WATCHGUARD OR FROM PRODUCT LIABILITY, STRICT LIABILITY OR OTHER THEORY, AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE TO, OR CAUSED BY OR CONTRIBUTED TO BY, THE PRODUCT).

4. LIMITATION AND LIABILITY. WATCHGUARD'S LIABILITY (WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT) OR OTHER THEORY) WITH REGARD TO ANY PRODUCT WILL IN NO EVENT EXCEED THE PURCHASE PRICE PAID BY YOU FOR SUCH PRODUCT. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF ANY AGREED REMEDY. IN NO EVENT WILL WATCHGUARD BE LIABLE TO YOU OR ANY THIRD PARTY (WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT) OR OTHER THEORY) FOR COST OF COVER OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF PROFITS, BUSINESS, OR DATA) ARISING OUT OF OR IN CONNECTION WITH THIS WARRANTY OR THE USE OF OR INABILITY TO USE THE PRODUCT, EVEN IF WATCHGUARD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF ANY AGREED REMEDY.

5. MISCELLANEOUS PROVISIONS. This Warranty will be governed by the laws of the state of Washington, U.S.A., without reference to its choice of law rules. The provisions of the 1980 United Nations Convention on Contracts for the International Sales of Goods, as amended, shall not apply. You agree not to directly or indirectly transfer the Product or associated documentation to any country to which such transfer would be prohibited by the U.S. Export laws and regulations. If any provision of this Warranty is found to be invalid or unenforceable, then the remainder shall have full force and effect and the invalid provision shall be modified or partially enforced to the maximum extent permitted by law to effectuate the purpose of this Warranty. This is the entire agreement between WatchGuard and you relating to the Product, and supersedes any prior purchase order, communications, advertising or representations concerning the Product AND BY USING THE PRODUCT YOU AGREE TO THESE TERMS. IF THE PRODUCT IS BEING USED BY AN ENTITY, THE INDIVIDUAL INDICATING AGREEMENT TO THESE TERMS BY USING THE PRODUCT REPRESENTS AND WARRANTS THAT (A) SUCH INDIVIDUAL IS DULY AUTHORIZED TO ACCEPT THE WARRANTY ON BEHALF OF THE ENTITY AND TO BIND THE ENTITY TO THE TERMS OF THIS WARRANTY; (B) THE ENTITY HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THE WARRANTY AND PERFORM ITS OBLIGATIONS UNDER THE WARRANTY AND; (C) THE WARRANTY AND THE PERFORMANCE OF THE ENTITY'S OBLIGATIONS UNDER THE WARRANTY DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH THE ENTITY IS A PARTY. No change or modification of the Warranty will be valid unless it is in writing and is signed by WatchGuard.

Firmware Version: 7.1
Part Number: 1776-0000
Guide Version: 7.1-beta1

Abbreviations Used in this Guide

3DES	Triple Data Encryption Standard
BOVPN	Branch Office Virtual Private Network
DES	Data Encryption Standard
DNS	Domain Name Service
DHCP	Dynamic Host Configurationl Protocol
DSL	Digital Subscriber Line
IP	Internet Protocol
IPSec	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
MAC	Media Access Control
MUVPN	Mobile User Virtual Private Network
NAT	Network Address Translation
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
TCP	Transfer Control Protocol
UDP	User Datagram Protocol
URL	Universal Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network
WSEP	WatchGuard Security Event Processor

Contents

Introduction to Network Security

Congratulations on your purchase of the WatchGuard Firebox® X Edge. Your new security device provides peace of mind when countering today's network security threats.

To provide context for the many features described throughout this user guide, this chapter explains basic concepts of networking and network security.

Network Security

Although the Internet puts a tremendous volume of information at your fingertips, it also presents risks by exposing your network to attackers. Network security is the process of preventing and detecting unauthorized use of your computer or network. Prevention measures help you to stop intruders from accessing any part of your computer system.

Although you may not consider anything on your computer "top secret," you should still be very concerned about security. If you aren't careful, intruders can take malicious actions such as use your computer to attack other computer systems, send forged e-mail from your computer, or steal your financial information. They can also damage your computer by reformatting your hard drive or changing your data.

Computer security must always be kept up-to-date. Intruders are always discovering new vulnerabilities to exploit in computer software.

About Networks

A network is a connected group of computers and other devices. It can consist of anything from two computers connected by a serial cable to thousands of computers connected by high-speed data communication links located throughout the world.

A *Local Area Network* (LAN) is a group of computers linked electronically to form a common work environment. This facilitates the sharing of applications and data, and is especially important when a group of people need to work together on one project.

A *Wide Area Network* (WAN) involves computers separated by significant distances, such as those located in different buildings.

Clients and servers

The terms *client* and *server* are used to describe individual computers that are part of a network. A server is a computer that makes its resources available to the network and responds to the commands of a client. Examples of a server's shared resources are files (a file server), printers (a print server), and processing power (an application server). A client is a computer that uses the resources made available by the server.

Connecting to the Internet

You have a number of options for connecting to the Internet. High-speed Internet connections, such as cable modem or Digital Subscriber Line (DSL), are referred to as broadband connections. *Bandwidth* describes the relative speed of an Internet connection, such as 1 Megabit per second (Mbps).

You can use a cable modem to connect to the Internet via the cable TV network. The cable modem usually has an Ethernet LAN connection to the computer, and it is capable of speeds in excess of 5 Mbps.

Typical speeds tend to be lower than the maximum, however, because cable providers turn entire neighborhoods into LANs that

share the same bandwidth. Because of this "shared-medium" topology, cable modem users might experience somewhat slower network access during periods of peak demand, and can be more susceptible to certain types of attacks more than users with other types of connectivity.

Digital Subscriber Line (DSL) Internet connectivity, unlike cable modem-based service, provides the user with dedicated bandwidth. However, the maximum bandwidth available to DSL users is usually lower than the maximum cable modem rate because of differences in their respective network technologies. Also, the "dedicated bandwidth" is dedicated only between your home or office and the DSL provider's central office. The provider offers little or no guarantee of bandwidth across the Internet.

Internet Service Providers (ISP) are companies that provide access to the Internet.

Protocols

You will often hear the term protocol. A *protocol* is a specification that allows computers to communicate across a network. In a way, protocols define the grammar that computers use to communicate with each other.

The standard protocol whenever you connect to the Internet is called Internet Protocol (IP). This protocol can be thought of as the common language of computers on the Internet.

A protocol also defines how data is assembled and transmitted through a network. The most frequently used protocols are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). Other IP protocols are less commonly used.

TCP/IP is the basic protocol used by computers connected to the Internet. TCP/IP involves certain settings that you need to know when setting up your Firebox X Edge. For more information on TCP/IP, see "Finding your TCP/IP properties" on page 13.

How Information Travels on the Internet

The data that is sent through the Internet is divided into units called packets. When you send a file from one place to another on the

Internet, the file is divided into chunks of data. Each chunk, or packet, is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file. To make sure that the packets are received at the destination, information is added to the packets.
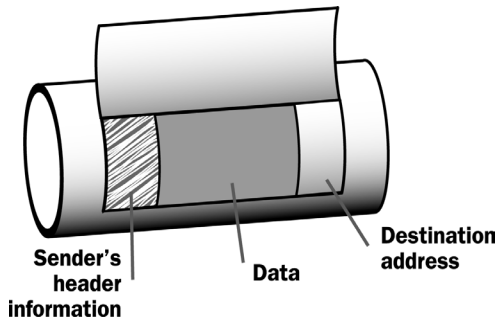
Data packet

The TCP and IP protocols are used for sending and receiving these packets. TCP disassembles and reassembles the data; for example, data that may consist of an e-mail message or a program file. IP adds information to the packets that includes the destination and the handling requirements.
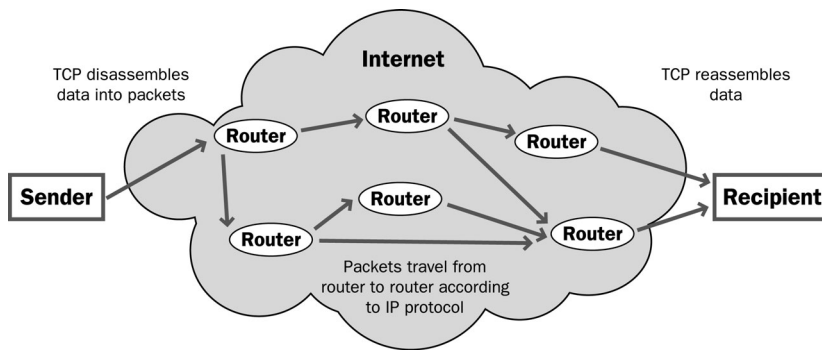
Packets traveling on the Internet

IP Addresses

IP addresses are like street addresses—when you want to send some information to someone, you must first know his or her address. Similarly, when a computer connected to the Internet needs to send data to another computer, it must first know its IP address.

Each computer on the Internet has its own unique IP address. An IP address consists of four sets of numbers separated by decimal points. Examples of IP addresses are:

- 192.168.0.11
- 10.1.20.18
- 208.15.15.15

A firewall device such as the Firebox® X Edge is also a computer and therefore has its own IP address.

Network addressing

Your ISP assigns IP addresses, which are a requirement to connect to the Internet. The assignment of IP addresses is *dynamic* or *static*.

Static IP addressing occurs when an ISP permanently assigns one or more IP addresses for each user. These addresses do not change over time. However, if a static address is assigned but not in use, it is effectively wasted. Because ISPs have a limited number of addresses allocated to them, they sometimes need to make more efficient use of their addresses.

Dynamic IP addressing allows the ISP to use their address space more efficiently. Using dynamic IP addressing, the IP addresses of individual user computers may change over time. If a dynamic address is not in use (the user is not connected to the network), it can be automatically reassigned to another computer as needed.

Your ISP can tell you how their system assigns IP addresses.

About DHCP

Most ISPs make dynamic IP address assignments through (Dynamic Host Configuration Protocol (DHCP). When a computer connects to the network, a DHCP server at the ISP assigns that computer an IP address. The manual assignment of IP addresses is not necessary when using DHCP.

About PPPoE

Some ISPs assign the IP addresses through Point-to-Point Protocol over Ethernet (PPPoE). PPPoE emulates a standard dial-up connection to provide some of the features of Ethernet and PPP. This system allows the ISP to use the billing, authentication, and security systems designed for dial-up, DSL modem, and cable modem service.

Domain Name Service (DNS)

If you don't know a person's street address, you can look it up in the telephone directory. On the Internet, the equivalent to a telephone directory is the Domain Name Service, or DNS. You probably use DNS all the time without knowing it. Whenever you use a ".com" address such as www.mysite.com (which is actually the site's *domain name*) to visit an Internet site, you are using DNS. When you type the .com address into your Internet browser (such as Internet Explorer or Netscape), your computer asks its DNS server for the actual IP address of the site.

A URL (Uniform Resource Locator) identifies each IP address on the Internet. An example of a URL is:

http://www.watchguard.com/

Services

As the name implies, a service provides some kind of useful function for you on the computer, such as exchanging e-mail or transferring files from one computer to another through the network. These services are based on specific protocols. Commonly used Internet services are:

- World Wide Web access uses Hypertext Transfer Protocol (HTTP)
- E-mail uses Simple Mail Transfer Protocol (SMTP)
- File transfer uses File Transfer Protocol (FTP)
- Resolving a domain name into an Internet address uses Domain Name Service (DNS)
- Remote terminal access uses Telnet or Secure Shell

Although some services are essential, they can also be a security risk. To send and receive data, you must "open a door" in your computer, which makes your network vulnerable. One of the most common ways networks are broken into is by intruders exploiting services.

Ports

On computers and other telecommunication devices, a port is a specific place for physically connecting another device, usually with a socket and plug. A computer usually has one or more serial ports and one parallel port. The serial port supports sequential, one bit-at-a-time transmission to devices such as scanners, and the parallel port supports multiple-bit-at-a-time transmission to devices such as printers.

Computers also have ports that are not physical locations. These ports are "logical connection places" for programs or applications on a computer in a network. Some applications, such as HTTP, have ports with preassigned numbers. These are known as "well-known ports." Other application processes are assigned port numbers dynamically for each connection. When a service is initially started, it is said to "bind" to its designated port number.

Every Internet service using TCP is identified by a unique port number. When a client initiates a connection to a server, it chooses to connect to, say, port 25 on the remote machine. Port 25 is assigned to the SMTP protocol which is the service of delivering electronic mail.

Most services are assigned a port number in the range from 0 to 1024, but the valid port numbers range from 0 to 65535.

Firewalls

A *firewall* divides your internal network from the Internet to reduce this danger. The computers on the "trusted" (internal) side of a firewall are protected. The illustration below shows how a firewall physically divides the trusted network (your computers) from the Internet.

INTERNET

DSL OR CABLE MODEM

FIREBOX X EDGE

PROTECTED COMPUTERS
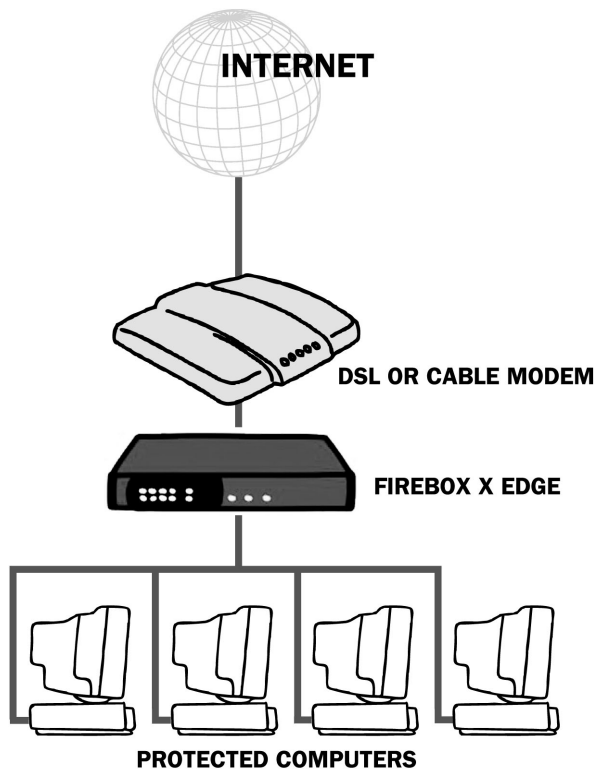
Firewalls allow the user to define access policies for the Internet traffic going to the computers they are protecting. Many also provide the ability to control what services or ports the protected computers are able to access on the Internet (outbound access). Most firewalls intended for home use come with pre-configured security policies from which the user chooses, and some—such as the Firebox X Edge—allow the user to customize these policies for their specific

needs.
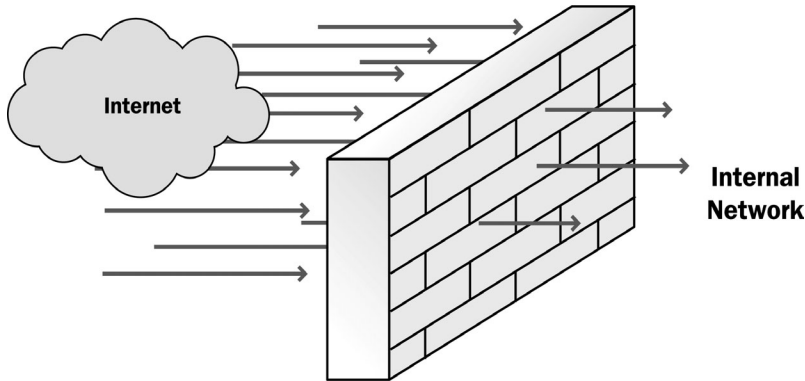
Firewalls are implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Firebox® X Edge and Your Network

The Firebox® X Edge controls all traffic between the external network (the Internet) and the trusted network. The Edge also supports an optional network to extend the protection of the firewall to include telecommuters on a separate network. All suspicious traffic is stopped. The rules and policies that identify the suspicious traffic are described in Chapter 5, "Configuring Firewall Settings."

Designed for small and remote offices with modest in-house security expertise, the Firebox X Edge is a high-performance security device that simply plugs in between your cable, DSL, or ISDN router and your network.

The Web-based user interface of the Firebox X Edge intuitive and straight-forward. You don't need additional security expertise to install and manage your firewall. Because you can manage your network securely from anywhere, at any time, you have more time and resources to focus on your business.

Installing the Firebox® X Edge

To install the WatchGuard® Firebox® X Edge in your network, you must complete these steps:

- Identify and record the TCP/IP properties for your Internet connection.
- Disable the HTTP proxy properties of your Web browser.
- Connect the Firebox X Edge to your network.
- Enable your computer for DHCP.
- Activate the LiveSecurity® Service.
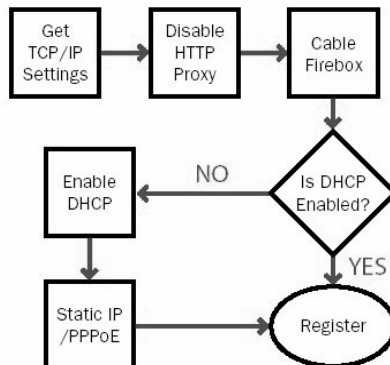
Package Contents

Make sure that the package for your Firebox® X Edge includes this User Guide and these items:

- The Firebox X Edge *QuickStart Guide*
- A LiveSecurity® Service activation card
- A Hardware Warranty Card
- An AC adapter (12 V)
- Power cable clip, to attach to the cable and connect to the side of the Edge. This releases tension on the power cable.
- One straight-through Ethernet cable
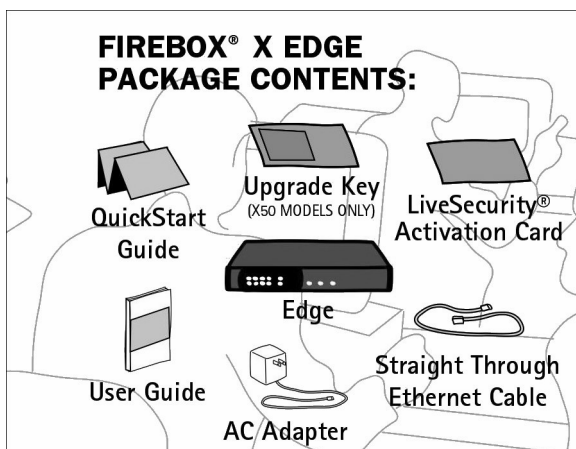
Installation Requirements

The other installation requirements are:

- A computer with a 10/100BaseT Ethernet I/O network interface card.
- A Web browser. You must use Netscape 7.0 (or later), Internet Explorer 6.0 (or later), or an equivalent browser.
- The serial number of the Firebox X Edge you see on the bottom of the device.
  You use the serial number to register the Edge.

- An Internet connection that operates.

   The external network connection can be a cable or DSL modem with a 10/100BaseT port, an ISDN router, or a direct LAN connection. If the Internet connection does not operate, speak to your Internet Service Provider (ISP).

Identifying Your Network Settings

You use an Internet Service Provider (ISP) to connect to the Internet. These ISPs give all computers an Internet Protocol (IP) address. An ISP can give you a static or dynamic IP address. A static address is an address that stays the same. A dynamic address is an address that can change each time you connect to the Internet. When you close a dynamic Internet connection, the dynamic address goes to the list of available addresses.

Your ISP gives you an IP address using one of these:

- Static: Web servers, FTP Web sites, and other Internet resources that must have an address that cannot change get static a IP addresses.

- DHCP: ISPs use the Dynamic Host Configuration Protocol (DHCP) to give you a dynamic IP address. Each time you connect to the ISP, a DHCP server can give you a different IP address.

- PPPoE: ISPs use Point-to-Point Protocol over Ethernet (PPPoE) to give you a dynamic IP address or a static IP address. A user name and passphrase are necessary for PPPoE.

An ISP can also give a network mask (netmask) to a computer. A netmask is a string of bits that "mask" one part of an IP address. You use a netmask to divide your network into smaller units, and creating added destinations to which you can send routed traffic.

Read your DSL or cable modem instructions or speak to your ISP to learn if you have a dynamic IP address or a static IP address.

Finding your TCP/IP properties

Transmission Control Protocol/Internet Protocol (TCP/IP) is the primary protocol computers use to connect to the Internet. To use TCP/IP, your computer must have an IP address and information about the computer network of your ISP. You must have this information to install your Firebox X Edge.

NOTE

If your ISP gives your computer an IP address of 10.0.0.0/8 or one that starts with 192.168 or 172.16 to 172.31, then your ISP uses network address translation (NAT). You must get a public IP address and disable NAT on your intranet router for full functionality. Get instructions from your ISP.

Your TCP/IP Properties Table

TCP/IP Property		Value
IP Address		. . .
Subnet Mask		. . .
Default Gateway		. . .
DHCP Enabled		Yes No
DNS Server(s)	Primary	. . .
	Secondary	. . .

To find your TCP/IP properties, use the instructions for your computer operating system.

Microsoft Windows 2000 and Windows XP

1   Click **Start** > **Programs** > **Accessories** > **Command Prompt**.

2   At the MS-DOS prompt, type `ipconfig /all` and then press **Enter**.

3   Record the values in the Your TCP/IP Properties Table on page 14.

4   Close the window.

Microsoft Windows NT

1   Click **Start** > **Programs** > **Command Prompt**.

2   At the MS-DOS prompt, type `ipconfig /all` and then press **Enter**.

3   Record the values in the Your TCP/IP Properties Table on
     page 14.

4   Close the window.

Microsoft Windows 98 or ME

1   Click **Start** > **Run**.

2   At the MS-DOS prompt, type `winipcfg` and then press **Enter**.

3   Click **OK**.

4   Select the **Ethernet Adapter**.

5   Record the values in the Your TCP/IP Properties Table on
     page 14.

6   Click **Cancel**.

Macintosh

1   Click the **Apple** menu > **Control Panels** > **TCP/IP**.

2   Record the values in the Your TCP/IP Properties Table on
     page 14.

3   Close the window.

Other operating systems (Unix, Linux)

1   Read your operating system guide to locate the TCP/IP settings.

2   Record the values in the Your TCP/IP Properties Table on
     page 14.

3   Exit the TCP/IP configuration screen.

Disabling the HTTP Proxy Setting

A proxy is a computer procedure that receives and examines packet
headers and packet content. If the proxy finds packet headers or
packet contents that do not obey the proxy rules, those packets are
denied, blocked, or stripped. The proxy policy monitors and controls
traffic to protect your network from the Internet.

Many Web browsers use the HTTP proxy to monitor incoming Inter-
net traffic. When this proxy is enabled, you can see Web pages on
the Internet, but you cannot see Web pages in other locations.
Because you must see pages that are stored or saved on the Firebox
X Edge to complete the installation procedure, you must disable this
proxy temporarily.

You can use the instructions below to disable the HTTP proxy in Netscape or Internet Explorer. If you are using a different browser, try using the browser Help system to find the necessary information. Many opensource browsers automatically disable the HTTP proxy feature.

Netscape

1   Open Netscape.

2   Click **Edit > Preferences.**
    The Preferences window appears.

3   A list of options appears at the left side of the window. Click the arrow symbol to the left of the **Advanced** heading to expand the list.

4   Click **Proxies**.

5   Make sure the **Direct Connection to the Internet** option is selected.

6   Click **OK.**

Internet Explorer

1   Open Internet Explorer.

2   Click **Tools > Internet Options**.
    The Internet Options window appears.

3   Click the **Advanced** tab.

4   Scroll down the page to **HTTP 1.1 Settings**.

5   Clear all of the checkboxes.

6   Click **OK.**

Connecting the Firebox X Edge
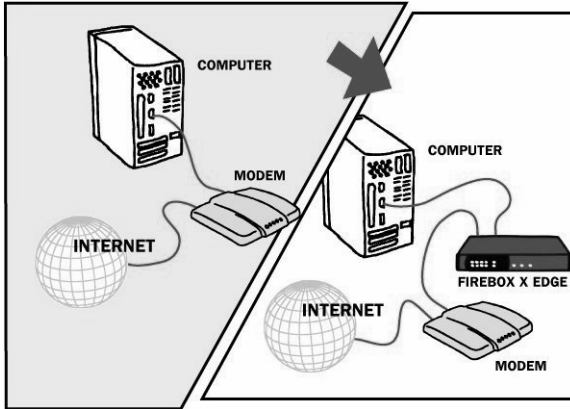
Use this procedure to connect your Firebox® X Edge Ethernet and power cables:

1   Shut down your computer.

2   If you use a DSL or cable modem to connect to the Internet, disconnect its power supply.

3   Find the Ethernet cable between the modem and your computer. Disconnect this cable from your computer and connect it to the Edge external interface (WAN 1).
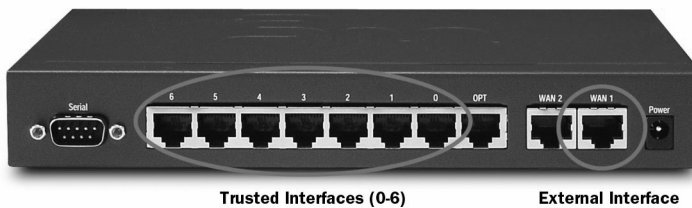
4   Find the Ethernet cable supplied with your Edge. Connect this cable to a trusted interface (0-6) on the Edge. Connect the other end of this cable to the Ethernet interface of your computer.

5   If you use a DSL or cable modem, connect its power supply.

---

6   Find the AC adapter supplied with your Edge. Connect the AC adapter to the Edge and to a power source.

The Edge power indicator light comes on and the external interface indicator lights flash and then come on. The Edge is ready.

─────────────── **NOTE** ───────────────

Use only the Firebox X Edge AC adapter.

───

7   When the Edge is ready, start your computer.

Cabling the Firebox X Edge for more than seven devices

Although the Firebox X Edge has only seven numbered Ethernet ports (labeled 0-6), you can connect more than seven devices. Use one or more network hubs to make more connections.

The maximum number of devices that can connect to the Internet at the same time is set by model. For example, the Firebox X5 has a five-session license. There can be more than five devices on the trusted network, but the Edge allows only five Internet connections at the same time.

The Edge uses a session when it makes a connection between a computer on the trusted interface and a computer on the external interface. The Edge releases the session when:

•   The session reaches the idle timeout limit

•   The session reaches the maximum time limit

•   The Edge administrator uses the Firebox Users page to end the session

•   The user ends the session by closing all browser windows

•   The Edge restarts.

For more information, see the FAQ:

https://www.watchguard.com/support/AdvancedFaqs/sogen_seatlimit.asp

License upgrades are available from your reseller or from the WatchGuard Web site:

http://www.watchguard.com/sales/buyonline.asp

To connect more than seven devices to the Edge, you need:

•   An Ethernet 10/100Base TX hub or switch

•   A straight-through Ethernet cable, with RJ-45 connectors, for each computer

- A straight-through Ethernet cable to connect each hub to the Firebox X Edge.

To connect more than seven devices to the Firebox X Edge:

1 Shut down your computer. If you connect to the Internet through a DSL modem or cable modem, disconnect the power supply from this device.

2 Disconnect the Ethernet cable that runs from your DSL modem, cable modem, or other Internet connection to your computer. Connect the Ethernet cable to the WAN port on the Firebox X Edge.

   The Firebox X Edge is connected directly to the modem or other Internet connection.

3 Connect one end of the straight-through Ethernet cable supplied with your Firebox X Edge to one of the seven numbered Ethernet ports (labeled 0-6) on the Edge. Connect the other end to the uplink port of the Ethernet hub or switch.

   The Firebox X Edge is connected to the Internet and your Ethernet hub or switch.

4 Connect an Ethernet cable between each of the computers and an uplink port on the Ethernet hub, and make sure the link lights are lit on both devices when powered back on.

5 If you connect to the Internet through a DSL modem or cable modem, reconnect the power supply to this device. The indicator lights flash and then stop. The modem is ready for use.

6 Attach the AC adapter to the Firebox X Edge. Connect the AC adapter to a power supply.

7 Restart your computer.

   If you get a message that says your operating system has no network connection, shut down all equipment and make sure all devices are connected properly.

8 Start your Internet browser.

9 Type https://192.168.111.1/ into the URL entry field of your browser and press Enter.

10 Follow the steps in the QuickSetup Wizard to configure your Firebox X Edge.

If your ISP uses static IP addressing, or uses PPPoE, then do the following additional steps:

1   From your Web browser, select **File > Open Location**, type https://192.168.111.1/ into the URL entry field of your browser, and press **Enter.** Log on using the default user name (admin) and password (admin).

2   From the navigation bar, expand **Network** (click the plus sign) and select **External**.

3   From the **Configuration Mode** drop-down list, select either **Manual Configuration** (for static IP addressing) or **PPPoE Client**.

Connecting to the System Configuration Pages

Use a Web browser to connect to the Firebox® X Edge system configuration pages. The first time you connect to the Edge configuration pages, the End User License Agreement (EULA) appears. To continue, you must accept the agreement. You must also set the administrator password.

A factory default Edge allows HTTP traffic on port 80. After you set the administrator password, the Edge uses only secure HTTP (HTTPS) on port 443 for system configuration.

For your computer to connect to the Edge, you must choose one of these options:

•   Get a dynamic IP address from the Edge using DCHP

•   Set a static IP address within the default trusted interface address range
    The default trusted interface IP address is 192.168.111.1/24.

For more information on network addressing, see "IP Addresses" on page 5.

Setting your computer to use DHCP

This procedure sets a computer with the Windows XP operating system to use DHCP. If your computer does not use Windows XP, read

the documentation for instructions to set your computer to use DHCP.

1   Click **Start > Control Panel**.
    The Control Panel window appears.

2   Double-click the **Network Connections** icon.

3   Double-click the **Local Area Connection i**con.

4   Double-click the **Internet Protocol (TCP/IP)** item.
    The Internet Protocol (TCP/IP) Properties dialog box appears.

5   Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** options.

6   Click **OK** to close the **Internet Protocol (TCP/IP) Properties** dialog box.

7   Click **OK** to close the **Local Area Network Connection Properties** dialog box. Close the **Network Connections** and **Control Panel** windows.
    Your computer is now connected to the Firebox X Edge.

Setting your computer with a static IP address

This procedure sets a computer with the Windows XP operating system to a static IP address. If your computer does not use Windows XP, read the documentation for instructions to set your computer to use DHCP. You must use an IP address on the same network as the Firebox X Edge trusted interface.

1   Click **Start > Control Panel**.
    The Control Panel window appears.

2   Double-click the **Network Connections** icon.

3   Double-click the **Local Area Connection** icon.

4   Double-click the **Internet Protocol (TCP/IP)** item.
    The Internet Protocol (TCP/IP) Properties dialog box appears.

5   Select the **Use the following IP address** option.

6   In the IP address field, type an IP address on the same network as the Edge trusted interface. We recommend 192.168.111.2.
    The default trusted interface network is 192.168.111.0/24. The last number can be between 2 and 254.

7   In the **Subnet Mask** field, type 255.255.255.0.

8   In the **Default Gateway** field, type the IP address of the Edge
    trusted interface.
    The default Edge trusted interface address is 192.168.111.1.

9   Click **OK** to close the **Internet Protocol (TCP/IP) Properties**
    dialog box.

10 Click **OK** to close the **Local Area Network Connection
    Properties** dialog box. Close the **Network Connections** and
    Control Panel windows.
    Your computer is now connected to the Firebox X Edge.

Browsing to the System Status page

Use a Web browser to connect to the Edge and then change the
network settings.

1   Open your Web browser.
    If this is the first connection to the Edge, the End User License
    Agreements appears. You must accept the agreement and set your
    administrator password to continue.

2   In the Address bar, type the Edge trusted interface IP address
    which is **https://192.168.111.1** for a new Edge. Press the **Enter**
    key.

Configuring the External Interface

Your Internet Service Provider (ISP) uses DHCP, PPPoE, or static IP addressing to identify your computer on their network. After you connect the Edge, you must configure the external interface with the information from your ISP.

Setting the Edge to use DHCP

A new Edge uses DHCP to get an IP address for the external interface. If your ISP uses DHCP addressing to identify your computer on their network, it is not necessary to make a configuration change unless the ISP gives you a DHCP ID or name. If necessary, use this procedure to set the DHCP ID or name:

1   Open your Web browser. Browse to the System Status page at https://192.168.111.1.
    Type the URL in the Address bar of your browser and press the [Enter] key.

2   From the navigation bar on the left side, click the **+** symbol to the left of **Network**. Click **External**.

3   Use the **Configuration mode** drop-down list to select **DHCP Client**.

4   In the **Optional DHCP Identifier** field, type the DHCP name or ID you got from your ISP.

5   Click **Submit**.

```
Network
External Network Configuration
_____

Configuration Mode | DHCP Client        |▼|
             IP Address  192.168.54.54
           Subnet Mask  255.255.255.0
       Default Gateway  192.168.54.254
           Primary DNS  192.168.130.131
         Secondary DNS  192.168.130.245
     DNS Domain Suffix  wgti.net
  Optional DHCP Identifier |                    |

  [ Submit ]  [ Reset ]
```

Setting a Static IP Address

If your ISP uses static IP addressing, you must set the Edge external interface address. Use the information in the Your TCP/IP Properties Table on page 14 to do this procedure.

1   Open your Web browser. Browse to the System Status page at https://192.168.111.1.
    Type the URL in the Address bar of your browser and press the [Enter] key.

2   From the navigation bar on the left side, click the plus sign (**+)** to the left of **Network**. Click **External**.

3   Use the **Configuration mode** drop-down list to select **Manual Configuration.**

4   Type the IP address, subnet mask, and default gateway.

5   Type the IP addresses of the primary and secondary DNS servers.

6   Type the DNS domain suffix.

7   Click **Submit**.

Network
External Network Configuration

Configuration Mode	Manual Configuration ▼
IP Address	192.168.54.54
Subnet Mask	255.255.255.0
Default Gateway	192.168.54.254
Primary DNS	192.168.130.131
Secondary DNS	192.168.130.245
DNS Domain Suffix	wgti.net

Submit   Reset

Entering PPPoE settings

Many ISPs use Point to Point Protocol over Ethernet (PPPoE) because it is easy to merge with dial-up infrastructure. If your ISP uses PPPoE to give IP addresses, you must get more setup information.

PPPoE Address Settings

PPPoE Setting	Value
Login Name	
Domain	
Password	

For more information in PPPoE, see "About PPPoE" on page 6. To configure the Edge for PPPoE:

1   Open your Web browser and click **Stop**.
    Because the Internet connection is not configured, the browser cannot show your home page from the Internet. The browser can only open the configuration pages saved on the Edge.

2   Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
    The default IP address is: https://192.168.111.1

3   From the navigation bar at left, select **Network > External**.
    The External Network Configuration page opens.

4   From the **Configuration Mode** drop-down list, select **PPPoE Client**.

5 Type the PPPoE login name and domain as well as the PPPoE password supplied by your service provide in the applicable fields.

6 Type the time delay before inactive TCP connections are disconnected.

7 If appropriate, select the **Automatically restore lost connections** checkbox.

This option keeps a constant traffic flow between the Edge and the PPPoE server. Thus the Edge keeps the PPPoE connection open during a period of frequent packet loss. If the traffic flow stops, the Edge reboots, which frequently activates the connection. The ISP sees this constant traffic flow as a continuous connection. The ISP rules and billing policy control if you can use this option.

8 Select the **Enable PPPoE debug trace** checkbox to activate PPPoE debug trace.

This can assist WatchGuard Technical Support in troubleshooting PPPoE problems.

9 Click **Submit**.

Registering Your Edge and Activating LiveSecurity Service

After you install the Firebox® X Edge, you can register the Edge and activate your LiveSecurity® Service subscription. The LiveSecurity Service gives you threat alert notifications, security advice, free virus protection, software updates, technical support by Web or telephone, and access to online help resources and the WatchGuard user forum.

You must have a subscription to the LiveSecurity Service before you can get license keys for the upgrades that you purchase. To apply upgrades, you must log into LiveSecurity Service and enter your upgrade key. You get a *feature key* to activate the features on your Firebox X Edge.

You must have the serial number of your Firebox X Edge to register. The Edge serial number is on the bottom of the device. Record the serial number in the table below:

1 Register your Firebox X Edge with the LiveSecurity Service at the WatchGuard Web site:

http://www.watchguard.com/activate

────────────── **NOTE** ──────────────

To activate the LiveSecurity Service, your browser must have JavaScript enabled.

2   If you have a user profile on the WatchGuard Web site, enter your user name and password. If you have not registered before, you must create a user profile. To do this, follow the instructions on the Web site.

3   Record your LiveSecurity Service user profile information in the table below. Keep this information confidential.

WatchGuard User Profile

User name:	
Password:	
Serial Number:	

4   If a model upgrade key is included with your model, activate it by going to:
      http://www.watchguard.com/upgrade

5   Select your product and follow the instructions for product activation.

CHAPTER 3   Configuration and Management Basics

When you *configure* a Firebox, you make the WatchGuard® Firebox® X Edge appropriate for the specific security needs of your organization. This is your main task after you install your Firebox. You use Web pages inthe Firebox to create the configuration of the Firebox X Edge. You connect to these configuration pages with your Web browser.

You can also use the Firebox Web pages to create accounts, look at network statistics, and see the current configuration of the Firebox.

Read this chapter to learn basic information about the Firebox X Edge Web pages. Sections in later chapters have more detailed intructions. This chapter contains cross-references to those later sections.

Navigating the Configuration Pages

To configure your Firebox® X Edge, you use a Web browser such as Internet Explorer, Mozilla Firefox, or NetScape Navigator. You must first disable the HTTP Proxy feature. For more information, see "Disabling the HTTP Proxy Setting" on page 15.

In this User Guide, every procedure starts with a step to:

"Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge. The default IP address is https://192.168.111.1."

The purpose of the step is to open your Firebox system configuration pages. Your computer must be connected to the Firebox with an Ethernet cable. You can change the IP address of the trusted network from https://192.168.111.1 to an IP address of your choice. For more information, see "Configuring the Trusted Network" on page 50.

For example, if you use Internet Explorer to configure your Firebox:

1   Start Internet Explorer.

2   Click **File > Open**, type **https://192.168.111.1** in the text box next to the word **Open**, and then click **OK**.

    You can also type the URL directly into the Address bar and press the Enter key.

Using the navigation bar

On the left side of the System Status page is a navigation bar that you use to see other Firebox X Edge configuration and status pages.

System Status
Network
Firebox Users
Administration
Firewall
Logging
WebBlocker
VPN
Wizards
Authenticate User
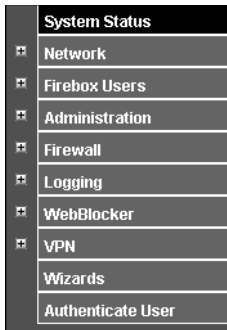
To see the main page for each area, click the appropriate menu item on the navigation bar. For example, to see how logging is currently configured for your Firebox and to see the current event log, click **Logging**.

Each area contains submenus that you use to configure various settings within that area. To see these submenus, click the plus sign (+) to the left of the area. For example, if you click the plus sign next to WebBlocker, the following submenu items appear: Settings, Profiles, Allowed Sites, Denied Sites, and Trusted Hosts.

This guide uses a series of arrow (>) symbols to show menu items that you expand or click. The menu names are in **bold**. For example, the command to open the Denied Sites page appears in the text as **WebBlocker > Denied Sites.**

Logging in and setting a password

The Firebox X Edge has no administrative password until you set one. To connect to the Firebox before it has a password:

1   Start your Internet browser.

2   Click **File > Open**, type **https://192.168.111.1** in the text box next to the word **Open**, and then click **OK**.

3   The End User License Agreement (EULA) appears. Read through it, and if you agree, accept the EULA.

4   Type your administrative password on the screen that appears. Type it again to confirm.

Configuration Overview

You use the Firebox X Edge system configuration pages to set up your Edge and make it work for your network and security requirements. This section gives a brief introduction to each category of pages and tells you which chapters in this *User Guide* contain detailed information about each feature.

Firebox System Status Page

The System Status page is the main configuration page of the Firebox X Edge. The center panel of the page shows information about the current settings. It also contains buttons so you can change these settings. This guide gives more detail on each setting in kater chapters.

Basic information on this page includes the following:

- Firebox components and their current versions
- The serial number of the device
- The status of key Firebox X Edge features
- The status of upgrade options
- Network configuration information
- Which external network (external or failover) is currently active. A green triangle appears next to the active network.
- Firewall configuration information
- A button to reboot the Firebox

Network Page

The Network page shows the configuration of each network inter-
face. It also shows any configured routes and has buttons you can
to change configurations and to see network statistics. For more
information, see Chapter 4, "Changing Your Network Settings."

```
Network

External Network

Configuration Method      Manual Configuration          [ Configure ]
IP Address                192.168.54.54
Subnet Mask               255.255.255.0
Gateway                   192.168.54.254
Primary DNS Server        192.168.130.131
Secondary DNS Server      192.168.130.245
Domain                    wgti.net
MAC                       00907F-0FDDDD

Trusted Network

IP Address                192.168.111.1                 [ Configure ]
Subnet Mask               255.255.255.0
MAC                       00907F-0FFFFF
DHCP Server               Disabled
                          0 addresses in use (251 max)
                          First address: 192.168.111.2

Optional Network

IP Address                192.168.112.1                 [ Configure ]
Subnet Mask               255.255.255.0
MAC                       Disabled
DHCP Server               Disabled
                          0 addresses in use (251 max)
                          First address: 192.168.112.2

Routes

Static Routes             No static routes defined.     [ Configure ]

[ View Statistics ]
```

Firebox Users Page

The Firebox Users page shows statistics on the active sessions and local user accounts. It also has buttons to close current sessions and to add, edit, and delete user accounts.

This page also shows the MUVPN client configuration files that are available for download. If you cannot yet use your Firebox for MUVPN clients, the page has a button for you to make your Firebox have MUVPN client support. For more information, see Chapter 11, "Managing the Firebox X Edge."

Firebox Users

Firebox User Settings

Firebox User accounts are disabled   [Configure]

    Restrict External Network access: Disabled
    Restrict VPN tunnel access: Disabled
    Enforce session idle time-out: Disabled
    Enforce maximum access time: Disabled
    Reset idle on Firebox X Edge access: Disabled

Periodic automatic global session time-out is disabled

Active Sessions

Active session count is 1 (maximum is 15).
The following sessions are currently active on this Firebox.

User	Host	Close
admin	192.168.111.2	✕

[Close All]

Local User Accounts

The following local user accounts have
been defined for this Firebox.   [Add...]

Name	Admin Level	WebBlocker	MUVPN	Edit	Delete
admin	Full	None	Disabled	⌨	⊘
new	None	restricted	Disabled	⌨	✕
sms	None	None	Disabled	⌨	✕

Secure MUVPN Client Configuration Files

The count of configured MUVPN clients is 0 (15 external).

Administration Page

The Administration page shows whether the Firebox uses HTTP or HTTPS for its configuration pages, whether VPN Manager access is enabled, and which upgrades are enabled. It has buttons to change configurations, add upgrades, and view the configuration file. For more information, see Chapter 11, "Managing the Firebox X Edge."

Administration

Administrative Options		
System Security	HTTPS mode	Configure
VPN Manager Access	Disabled	Configure
Upgrades		Upgrade
Installed Options:		
User Licenses	15	
Remote Gateways	Installed	
MUVPN Clients	Installed - license count 15	
WebBlocker	Installed	
WAN Failover	Installed	

View Configuration File

Firewall Page

The Firewall page shows the incoming and outgoing services, blocked sites, as well as other firewell settings. This page also has buttons to change these settings. For more information, see Chapter 6, "Configuring Firewall Settings."

Logging Page

The Logging page shows the current event log, status of WSEP and Syslog logging, and the system time. It also has buttons to change these settings and to set your system time so that it is the same as your local computer. For more information, see Chapter 7, "Configuring Logging."

Logging

Logging Options

WSEP Logging	Disabled	WSEP Log Host	None	Configure
Syslog Logging	Disabled	Syslog Host	0.0.0.0	Configure

System Time			Configure
Time Source	NTP Server	ntp3.cs.wisc.edu ntp1.cs.wisc.edu ntp-0.cso.uiuc.edu ntp-1.cso.uiuc.edu ntp-2.cso.uiuc.edu tick.cs.unlv.edu tock.cs.unlv.edu ntp1.gbg.netnod.se ntp2.gbg.netnod.se ntp1.mmo.netnod.se ntp2.mmo.netnod.se tick.greyware.com tock.greyware.com ntp1.sp.se ntp2.sp.se clock.via.net	
Time Zone	<Not Specified>		
DST	Disabled		
Current Time	2000-01-25-08:24:17		

Sync Time With Browser Now

Event Log

Time	Category	Message
2000-01-25-08:24:16	IP	allowed from 192.168.54.128 port 1577 to 192.168.54.54 port

WebBlocker Page

The WebBlocker page shows the WebBlocker settings, profiles, allowed sites, and denied sites. It also has buttons to change the current settings. For more information, see Chapter 8, "Configuring WebBlocker."

WebBlocker

WebBlocker Settings

Status	Disabled	Configure
Inactivity Time-out (minutes)	Not Set	
Authentication for Web Access	Not Required	

WebBlocker Profiles

Profile	Default Profile	Configure
Users	All Users	

Blocked Categories

Alcohol and Tobacco	UNKNOWN	Violence/Profanity	UNKNOWN
Illegal Gambling	UNKNOWN	Search Engines	UNKNOWN
Militant/Extremist	UNKNOWN	Sports and Leisure	UNKNOWN
Drug Culture	UNKNOWN	Sex Education	UNKNOWN
Satanic/Cult	UNKNOWN	Sex Acts	UNKNOWN
Intolerance	UNKNOWN	Full Nudity	UNKNOWN
Gross Depictions	UNKNOWN	Partial/Artistic Nudity	UNKNOWN

Allowed Sites

No allowed sites are defined.   Configure

Denied Sites

No denied sites are defined.   Configure

Trusted Hosts

No trusted hosts are defined.   Configure

VPN Page

The VPN page shows information on managed VPNs, manual VPN gateways, and echo hosts along with buttons to change the configuration of VPN tunnels. It also has a button for you to see statistics on active tunnels. For more information, see Chapter 9, "Configuring VPNs.

Wizards Page

The Wizards page shows the wizards available to help you quickly and easily set up key Firebox X Edge features:

- Network Interface Wizard
  Configure all interfaces, including WAN failover. For more information, see "Using the Network Setup Wizard" on page 45.
- Service Configuration Wizard
  Create a rule to filter network traffic between interfaces. For more information, see "Adding a custom policy using the wizard" on page 81.
- QuickSetup Wizard
  Set up your Firebox X Edge.
- Failover Setup Wizard
  Set up the failover network.
- Wireless Setup Wizard
  Set up the wireless interface.

What do you want to do?	Go!
Define a custom service for filtering network traffic between the External network and the Trusted and Optional networks.	🔧
Setup the primary network interfaces of the Firebox® X Edge.	🔧
Quick setup of the Firebox® X Edge.	🔧

Wizards

Updating Firebox X Edge Software

One benefit of your LiveSecurity® Service is ongoing software updates. As new threats appear and WatchGuard adds product enhancements, you receive alerts to let you know about new versions of your Firebox® X Edge software.

When you receive the alert, WatchGuard gives you instructions on how to download the software to your personal computer. After this download is complete, use the following instructions to update your Firebox software:

1   Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
    The default IP address is https://192.168.111.1.

2   At the bottom of the System Status page, click **Update**.
    The Administration Page appears with the End User License Agreement (EULA). You can also go to this page by selecting Administration > Update from the navigation bar at left.

3 Read the text of the EULA. If you agree, select the **I accept the above license agreement** checkbox.

4 Type the name of the file containing the new Firebox X Edge software in the **Select file** box or click **Browse** to find the file on your local computer.

5 Click **Update**.
   The Firebox makes sure the software package is a legimate software upgrade. It then copies the new software to the system and reboots. This can take 15 to 45 seconds. When the update is complete, the System Status page appears and shows the new version number.

Factory Default Settings

The term *factory default settings* refers to how the Firebox® X Edge is configured when you first receive it—before you have made any changes of your own to the configuration. The default network and configuration settings for the Firebox X Edge are as follows:

Trusted network
- The default IP address for the trusted network is 192.168.111.1. The subnet mask for the trusted network is 255.255.255.0.
- The Firebox X Edge is configured to give IP addresses to computers on the trusted network through DHCP. You can also give static addresses to computers in the trusted network with IP addresses in the 192.168.111.2–192.168.111.254 range.

External network
- The external network settings use DHCP.

Optional network
- The optional network is disabled.

Firewall settings
- All incoming services are blocked.
- An outgoing service allows all outbound traffic.
- All of the options on the Firewall Options page are disabled.

System Security
- The System Security is disabled. The system administrator name and system administrator passphrase are not set. All computers on the trusted network can see the configuration pages.
- Remote Management is disabled.

- VPN Manager Access is disabled.

- Remote logging is not configured.

WebBlocker

- The WebBlocker feature is disabled and the settings are not configured.

Upgrade Options

- The upgrade options are disabled until you type the license keys into the configuration page.

Resetting the Firebox to the factory default settings

You might have a reason to set the Firebox to the factory default settings. For example, you might be unable to correct a configuration problem and just want to "start over." Sometimes, a reset is your only choice: such as if the system security passphrase is unknown or the firmware of the Firebox X Edge is damaged by a power interruption.

You should have a copy of the most recent Firebox X Edge software on your local computer before you try to return to factory default settings.

Follow these steps to set the Firebox to the factory default settings:

1 Disconnect the power supply.

2 Hold down the **Reset** button, located on the front of the Firebox.

3 Connect the power supply while you continue to hold down the Reset button.

4 Continue to hold down the button until the red light on the front of the Firebox blinks in a steady pattern (about 15 seconds).

5 Disconnect the power supply.

6 Reconnect the power supply.
   The Power indicator is on and the reset is complete.

Rebooting the Firebox

You can reboot the Firebox® X Edge from a computer on the trusted network. You can also reboot the Firebox from a computer with the Internet to connect to the Firebox external interface.

The Firebox reboot cycle is up to 30 seconds. During the reboot cycle, the mode light on the front of the Firebox turns off and then turns on again.

Local reboot

You can locally reboot the Firebox X Edge either with the Web browser or by disconnecting the power supply.

Using the Web browser

1   Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
    The default IP address is: https://192.168.111.1
2   Click **Reboot**.

Disconnecting the power supply

Disconnect the Firebox power supply. After a minimum of 10 seconds, connect the power supply.

Remote reboot

You must configure the remote Firebox X Edge to send incoming HTTP (Web) or FTP traffic to the Firebox's trusted interface IP address if you want to use the following method to reboot it. For more information on how to configure the Firebox to receive incoming traffic, see "Configuring Incoming and Outgoing Policies" on page 65. Also, see the following FAQ for more information on configuring a Firebox X Edge to receive incoming traffic:

https://www.watchguard.com/support/tutorials/
stepsoho_remotemanage.asp

1   Type the external network IP address of the remote Firebox X
    Edge in your browser window to connect to its System Status
    page.

2   Click **Reboot**.

Changing Your Network Settings

A primary task to set up your WatchGuard® Firebox® X Edge is to configure the network IP addresses. At a minimum, you must configure the external network and the trusted network to let traffic flow through the Edge. You can also set up the optional interface. Many customers use the optional network for public servers. An example of a public server is a Web server.

You can use the Quick Setup Wizard to set up your network IP addresses. You can also manually set up or change your network IP addresses on the Network page.

Using the Network Setup Wizard

The easiest procedure to set up your network IP addresses is with the Network Setup Wizard.

1   To connect to the System Status page, type the IP address of the trusted network in the browser.
    The default IP address is: https://192.168.111.1.

2   From the navigation bar, select **Wizards**.

3   Next to **Setup the primary network interfaces of the Firebox X Edge**, click **Go**.

4   Work through the wizard, following the instructions on the screens. Steps associated with optional functionality you decide not to enable are automatically skipped by the wizard.

The Network Setup Wizard consists of the following steps:

Step 1: Welcome
The first screen describes the purpose of the wizard.

Step 2: Configure the External Interface of your Firebox
The next screen asks the method your ISP uses to set your IP address. For more information, see the next section in this guide, "Configuring the External Network."

Step 3a: Configure the External Interface for DHCP
On the next screen, type in your DHCP identification as provided by your ISP. For more information, see "If your ISP uses DHCP" on page 47.

Step 3b: Configure the External Interface for PPPoE
On the next screen, type in your PPPoE information as provided by your ISP. For more information, see "If your ISP uses PPPoE" on page 48.

Step 3c: Configure the External Interface with a static IP address
On the next screen, type in your static IP address information as provided by your ISP. For more information, see "If your ISP uses static IP addresses" on page 48.

Step 4: Configure the Trusted Interface of the Firebox
On the next screen, type the IP address of the trusted interface. For more information, see "Configuring the Trusted Network" on page 50.

Step 5: Change the User Name and Passphrase
The next screen enables you to set a username and passphrase for the Edge.

Step 6: The Network Setup Wizard is complete

Configuring the External Network

You must configure your external network manually if you choose not to use the Network Setup wizard.

When you configure the external network, set how your Internet Service Provider (ISP) gives an IP address to your Firebox. There are three methods to give IP addresses:

- **DHCP** - Network administrators use the Dynamic Host Configuration Protocol (DHCP) to give IP addresses to computers on their network automatically. With DHCP, your Firebox can receive a new external address each time it connects to the ISP network.

- **Static IP address** - Network administrators use static IP addresses to manually give an IP address to each computer on their network. Because more work is necessary with this procedure, an ISP frequently charges more for a static IP address. Static IP addresses are also known as manual addresses.

- **PPPoE** - Many ISPs use the Point to Point Protocol over Ethernet (PPPoE) to give IP addresses to each computer on their network. Frequently they use PPPoE with a dial-up network infrastructure.

To configure your Firebox® X Edge, you must know how it gets the IP address for the external interface. If you do not know the method, get the information from your ISP or corporate network administrator.

If your ISP uses DHCP

The default configuration sets the Firebox X Edge to get the external address information through DHCP. If your ISP uses DHCP, your Edge gets a new external IP address when it starts and connects to the ISP network.

For more information about DHCP, see "About DHCP" on page 5. To manually set your Firebox to use DHCP on the external interface:

1   To connect to the System Status page, type the IP address of the trusted network in the browser.
    The default IP address is: https://192.168.111.1

2   From the navigation bar, select **Network > External**.
    The External Network Configuration page appears.

3   From the Configuration Mode drop-down list, select **DHCP Client**.

4   Click **Submit**.

If your ISP uses static IP addresses

If your ISP uses static IP addresses, you must enter the address information into your Edge before it can send traffic through the external interface.

To set your Edge to use a static IP address for the external interface:

1   Use your browser to connect to the System Status page. From the navigation bar, select **Network > External**.
    The External Network Configuration page appears.

2   From the Configuration Mode drop-down list, select **Manual Configuration**.

Network
External Network Configuration

Configuration Mode	Manual Configuration ▼
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS	
Secondary DNS	
DNS Domain Suffix	

Submit   Reset

3   Type the IP address, Subnet Mask, Default Gateway, Primary DNS, Secondary DNS and DNS Domain Suffix into the related fields. Get this information from your ISP or corporate network administrator.
    If you completed the table on page 14, type the information from the table.
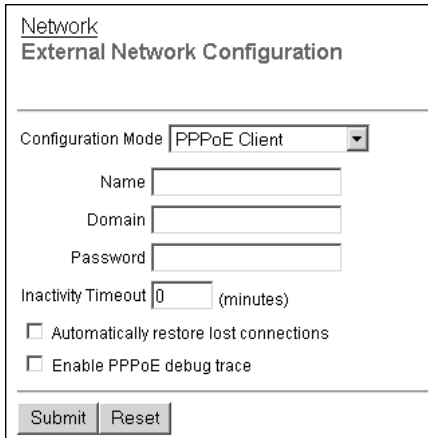
4   Click **Submit**.

If your ISP uses PPPoE

If your ISP uses PPPoE, you must enter the PPPoE information into your Firebox before it can send traffic through the external interface. For more information in PPPoE, see "About PPPoE" on page 6.

To set your Firebox to use PPPoE on the external interface:

1   Use your browser to connect to the System Status page. From the navigation bar, select **Network > External**.
The External Network Configuration page appears.

2   From the Configuration Mode drop-down list, select **PPPoE Client**.

3   Type the Name and Password in the related fields. Get this information from your ISP. If your ISP gives you a domain name, type it into the Domain field.
Most ISPs make the domain name section of the PPPoE name (e.g. *myname@ispdomain*). If you have a PPPoE name with this format, type the *myname* section in the Name field. Type the *ispdomain* section in the Domain field. Do not type the @ symbol. Some ISPs do not use the Domain.

4   Type the time before the Firebox disconnects inactive TCP connections.
We recommend a value of 20.

5   If necessary, select the **Automatically restore lost connections** check box.
The Firebox can keep a constant traffic flow to the PPPoE server. This flow keeps the PPPoE connection open when there is frequent packet loss. If the traffic flow stops, the Firebox restarts to make the connection again. The PPPoE server reads the constant traffic flow as a continuous connection. Many ISPs charge more if you use this option.

6   WatchGuard Technical Support uses the **Enable PPPoE debug trace** check box to troubleshoot PPPoE problems. With this

option on, the Firebox makes a file which you can send to Technical Support. Only use this option when Technical Support tells you. This option decreases Firebox performance.

7   Click **Submit**.

Configuring the Trusted Network

You must configure your trusted network manually if you choose not to use the Network Setup wizard.

You can use static IP addresses or DHCP for your trusted network. The Firebox® X Edge has a DHCP server to give IP addresses to computers on your trusted and optional networks. You can also change the IP address of the trusted network.

With a factory default Firebox, its DHCP server automatically gives IP addresses to computers on the trusted network. The trusted network starts with IP address 192.168.111.1. It is a "class C" network with a subnet mask of 255.255.255.0. The Firebox can give an IP address from 192.168.111.2 to 192.168.111.252. The factory default configuration uses the same DNS and domain name as it uses for the external interface. For more information, see "IP Addresses" on page 5.

If necessary, you can disable the Firebox DHCP server. The Firebox can forward the DHCP requests to a DHCP server on a different network. You can also use static IP addresses for the computers on your trusted network.

------------------------------ **NOTE** ------------------------------

You can make one or more changes to the trusted network, Submit each change, then Reboot only once to enable all of the changes. You must Reboot the Firebox to enable a change to the trusted network configuration.

You can make many changes and click Submit. Any change to the trusted network configuration All changes to the Trusted Network Configuration page require that you click Submit and then reboot the Firebox before they take effect.But you can make all the changes you want to make and then reboot just once when you are done.

Changing the IP address of the trusted network

If necessary, you can change the trusted network address. For example, if you connect two or more Firebox devices in a virtual private network, each Firebox must use a different trusted network address. For more information, see "What You Need to Create a VPN" on page 107.

To change the IP address of the trusted network:

1   To connect to the System Status page, type the IP address of the trusted network in the browser.
    The default IP address is: https://192.168.111.1

2   From the navigation bar, select **Network > Trusted**.
    The Trusted Network Configuration page appears.

3   Type the first address of the new network address range in the **IP Address** text field.

4   If necessary, type the new subnet mask.
    Most networks use 255.255.255.0 which includes 252 addresses.

Using DHCP on the trusted network

The DHCP Server option sets the Firebox X Edge to give IP addresses to the computers on the trusted network. When the Firebox receives a DHCP request from a computer on the trusted network, it gives the computer an IP address. A factory default Firebox has the DHCP Server option for the trusted interface on.

To use DHCP on the trusted network:

1   Use your browser to connect to the System Status page. From
    the navigation bar, select **Network > Trusted.**
    The Trusted Network Configuration page appears.

```
Network
Trusted Network Configuration
_____

                    IP Address  192.168.111.1
                   Subnet Mask  255.255.255.0
     □  Enable DHCP Server on Trusted Network
  First address for DHCP server  192.168.111.2
  Last address for DHCP server  192.168.111.252   [ DHCP Reservations... ]
            WINS Server Address  [            ]
             DNS Server Address  [            ]
   Secondary DNS Server Address  [            ]
              DNS Domain Suffix  [            ]
     □  Enable DHCP Relay
              DHCP relay server  [            ]
_____

  [ Submit ]  [ Reset ]
```

2   Select the **Enable DHCP Server on the Trusted Network** check
    box.

3   Type the first available IP address for the trusted network. Type
    last IP address.
    The IP addresses must be on the same network as the trusted IP address.
    For example, if your trusted IP address is 192.168.200.1, the IP addresses
    can be from 192.168.200.2 to 192.168.200.252.

4   Type the **WINS Server Address**, **DNS Server Primary Address**,
    DNS Server Secondary Address, and **DNS Domain Suffix** in the
    related fields.
    Use these field if you have a WINS or DNS server. If you do not enter a
    value, the Firebox uses the same values as those used for the external
    network.

5   Click **Submit.**

Setting trusted network DHCP address reservations

You can manually give an IP address to a specified computer on your trusted network. The Firebox identifies the computer by its MAC address.

1   Use your browser to connect to the System Status page. From the navigation bar, select **Network > Trusted**.
    The Trusted Network Configuration page appears.

2   Click the **DHCP Reservations** button.
    The DHCP Address Reservations page appears.

3   Type a static IP address in the **IP Address** field. The IP address must be on the trusted network.
    For example, if the trusted network starts with 192.168.111.1, you can enter 192.168.111.2 to 192.168.111.251.

4   Type the MAC address of the computer on the trusted network in the MAC Address field. Click **Add**.

5   Click **Submit**.

Configuring the trusted network for DHCP relay

One method to get IP addresses for the computers on the Firebox trusted network is to use a DHCP server on a different network. The Firebox can send a DHCP request to a DHCP server at a different location. It gives the reply to the computers on the Firebox trusted

network. This option lets computers in more than one office use the same network address range. This procedure makes the Firebox a *DHCP relay agent*.

To configure the Firebox as a DHCP relay agent for the trusted interface:

1   Use your browser to connect to the System Status page. From the navigation bar, select **Network > Trusted**.
    The Trusted Network Configuration page appears.

2   Select the **Enable DHCP Relay** check box.

3   Type the IP address of the DHCP server in the related field.

4   Click **Submit.**
    The Firebox restarts. If the Firebox can not connect to the DHCP server in 30 seconds, it uses its DHCP server to give IP addresses to computers on the trusted network.

Using static IP addresses for trusted computers

You can use static IP addresses for some or all of the computers on your trusted network. If you disable the DHCP server, you must manually configure the IP address and subnet mask of each computer. You can also configure specified computers with a static IP address. For example, this is necessary when a client server software application must use a static IP address for the server. Static IP addresses must be on the same network as the Firebox trusted interface.

To disable the Firebox DHCP server, clear the **Enable DHCP Server on the Trusted Network** check box on the Trusted Network Configuration page.

Adding computers to the trusted network

The Firebox X Edge can connect to one to seven trusted computers. You can use 10/100 BaseT Ethernet hubs or switches with RJ-45 connectors to connect more than seven computers. It is not necessary that the computers on the trusted network use the same operating system.

To add more than seven computers to the trusted network:

1   Make sure that each computer has a functional Ethernet card.

2   Set each computer to use DHCP. For more information, see "Setting your computer to use DHCP," on page 20.

3   Connect each computer to the network. Use the procedure "Cabling the Firebox X Edge for more than seven devices" on page 18.

4   Restart each computer.

Configuring the Optional Network

The optional network is an isolated network for less secure public resources. Many customers use the optional network for public computers such as a Web, e-mail, or FTP server. A factory default Firebox does not connect the trusted network to the optional network. While you can enable traffic between these networks, this procedure decreases security for the trusted network. For more information, see "Adding a Policy for the Optional Interface" on page 83.

You can use the Firebox® X Edge DHCP server or you can use static IP addresses for computers on the optional network. You can also change the IP address range of the optional network.

Many public servers must have a static IP address. For increased security, we recommend that you disable DHCP on the optional network. If it is necessary to protect your servers from Internet traffic, you can put your user computers on the optional network and your servers on the more secure trusted network.

───────── **NOTE** ─────────

You can make one or more changes to the optional network, Submit each change, then Reboot only once to enable all of the changes. You must Reboot the Firebox to enable a change to the optional network configuration.

Enabling the optional network

1   To connect to the System Status page, type the IP address of the trusted network in the browser.
The default IP address is: https://192.168.111.1

2   From the navigation bar, select **Network > Optional**.
The Optional Network Configuration page appears.

3   Select the **Enable Optional Network** check box.

Changing the IP address of the optional network

If necessary, you can change the optional network address. For example, you can isolate a wireless network from the trusted net-

work. A factory default Firebox has the trusted network and the optional network on 2 different subnets.

To change the IP address of the optional network:

1   To connect to the System Status page, type the IP address of the trusted network in the browser.
    The default IP address is: https://192.168.111.1

2   From the navigation bar, select **Network > Optional**.
    The Optional Network Configuration page appears.

3   Type the first address of the new network address range in the **IP Address** text field.

4   If necessary, type the new subnet mask.
    Most networks use 255.255.255.0 which includes 252 addresses.

Using DHCP on the optional network

The DHCP Server option sets the Firebox X Edge to give IP addresses to the computers on the optional network. When the Firebox receives a DHCP request from a computer on the optional network, it gives the computer an IP address. A factory default Firebox has the DHCP Server option for the optional interface off.

To use DHCP on the optional network:

1   Use your browser to connect to the System Status page. From
     the navigation bar, select **Network > Optional**.
     The Optional Network Configuration page appears.

Network
Optional Network Configuration

☐ Enable Optional Network
                         IP Address 192.168.112.1
                        Subnet Mask 255.255.255.0
☐ Enable DHCP Server on Optional Network
First address for DHCP server 192.168.112.2
Last address for DHCP server 192.168.112.252   DHCP Reservations...
            WINS Server Address
             DNS Server Address
Secondary DNS Server Address
            DNS Domain Suffix
☐ Enable DHCP Relay on Optional Network
              DHCP relay server
☐ Require encrypted MUVPN connections on this interface

Submit   Reset

2   Select the **Enable DHCP Server on the Optional Network** check
     box.

3   Type the first available IP address for the optional network. Type
     last IP address.
     The IP addresses must be on the same network as the optional IP
     address. For example, if your optional IP address is 192.168.112.1, the IP
     addresses can be from 192.168.112.2 to 192.168.112.252.

4   Type the **WINS Server Address**, **DNS Server Primary Address**,
     DNS Server Secondary Address, and **DNS Domain Suffix** in the
     related fields.
     Use these field if you have a WINS or DNS server. If you do not enter a
     value, the Firebox uses the same values as those used for the external
     network.

5   Click **Submit.**

Setting optional network DHCP address reservations

You can manually give an IP address to a specified computer on your optional network. The Firebox identifies the computer by its MAC address.

1   Use your browser to connect to the System Status page. From the navigation bar, select **Network > Optional**.
    The Optional Network Configuration page appears.

2   Click the **DHCP Reservations** button.
    The DHCP Address Reservations page appears.

3   Type a static IP address in the **IP Address** field. The IP address must be on the optional network.
    For example, if the optional network starts with 192.168.112.1, you can enter 192.168.112.2 to 192.168.112.251.

4   Type the MAC address of the computer on the optional network in the MAC Address field. Click **Add**.

5   Click **Submit**.

Configuring the optional network for DHCP relay

One method to get IP addresses for the computers on the Firebox optional network is to use a DHCP server on a different network. The Firebox can send a DHCP request to a DHCP server at a different

location. It gives the reply to the computers on the Firebox optional network. This option lets computers in more than one office use the same network address range. This procedure makes the Firebox a *DHCP relay agent*.

To configure the Firebox as a DHCP relay agent for the optional interface:

1   Use your browser to connect to the System Status page. From the navigation bar, select **Network > Optional**.
    The Optional Network Configuration page appears.

2   Select the **Enable DHCP Relay on Optional Network** check box.

3   Type the IP address of the DHCP server in the related field.

4   Click **Submit.**
    The Firebox restarts. If the Firebox can not connect to the DHCP server in 30 seconds, it uses its DHCP server to give IP addresses to computers on the optional network.

Using static IP addresses for optional computers

You can use static IP addresses for some or all of the computers on your optional network. If you disable the DHCP server, you must manually configure the IP address and subnet mask of each computer. You can also configure specified computers with a static IP address. For example, this is necessary when a client server software application must use a static IP address for the server. Static IP addresses must be on the same network as the Firebox optional interface.

To disable the Firebox DHCP server, clear the **Enable DHCP Server on the Optional Network** check box on the Optional Network Configuration page.

Adding computers to the optional network

The Firebox X Edge can connect to 1 optional computer. You can use 10/100 BaseT Ethernet hubs or switches with RJ-45 connectors to connect more than 1 computer. It is not necessary that the computers on the optional network use the same operating system.

To add more than 1 computers to the optional network:

1   Make sure that each computer has a functional Ethernet card.

2   Set each computer to use DHCP. For more information, see "Setting your computer to use DHCP," on page 20.

3   Connect each computer to the network. Use the procedure "Cabling the Firebox X Edge for more than seven devices" on page 18.

4   Restart each computer.

───────────────── **NOTE** ─────────────────
All changes to the Optional Network Configuration page require that you click Submit and then reboot the Firebox before they take effect. But you can make all the changes you want to make and then reboot just once when you are done.
───

You can either enable or disable the DHCP server on the optional network.

Requiring encrypted connections

You can set the optional interface to use only encrypted connections. Frequently a customer uses this option to make a secure wireless network. The wireless connections use the Mobile User VPN client. The client encrypts all traffic from the optional interface to the Firebox. A "drive-by" hacker can not read the encrypted traffic on the wireless network.

Making Static Routes

You can configure the Firebox to send specified traffic to different parts of the Firebox® X Edge trusted network connected by a router or switch. Use the Routes page to make a static route:

1   To connect to the System Status page, type the IP address of the trusted network in the browser.
The default IP address is: https://192.168.111.1

2   From the navigation bar, select **Network > Routes**.
     The Routes page appears.
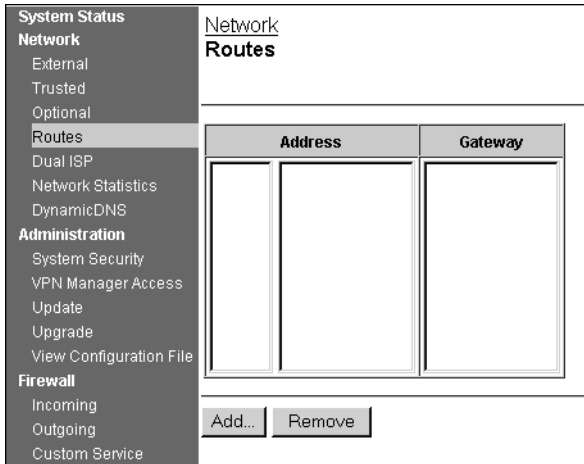
3   Click **Add**.
     The Add Route page appears.
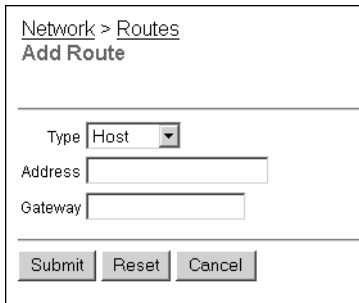
4   From the **Type** drop-down list, select either **Host** or **Network**.
     A host is 1 computer. A network is more than one computer which use a
     range of IP addresses.

5   Type the destination IP address and the gateway in the related
     fields.
     The Gateway is the ylocal interface of the router.

6   Click **Submit**.

To remove a static route, click the IP address and click **Remove.**

Viewing Network Statistics

The Firebox® X Edge Network Statistics page shows information about the performance. Network administrators frequently use this page to troubleshoot a problem with the Firebox or network.

1   To connect to the System Status page, type the IP address of the trusted network in the browser.
    The default IP address is: https://192.168.111.1

2   From the navigation bar, select **Network > Network Statistics**.
    The Network Statistics page appears.

```
Network
Statistics


IP

IP:     Up for 42 minutes 44 seconds
        Network Buffers Allocated/Total (-4913/100) Memory Total/Largest Block (21062352/20739312
        Sockets Allocated/Total (7/80) NAT Ports Avail (7000)
        RAM Disk Available (514048 bytes 96%) Flash Disk Available (129578 bytes 98%)
        Tx: packets (841)
        Rx: packets (1055) hdr Err(309) delivered (746)


External Network

eth0:   Link encap:Ethernet  HWaddr 00:90:7f:0f:dd:dd inet addr:192.168.54.54
        RX packets:904 errors:0 bcast:4096 disc:0 unk:0
        TX packets:887 errors:0 bcast:0


Trusted Network

eth1:   Link encap:Ethernet  HWaddr 00:90:7f:0f:ff:ff inet addr:192.168.111.1
        RX packets:0 errors:0 bcast:0 disc:0 unk:0
        TX packets:0 errors:0 bcast:0
```

Registering with the Dynamic DNS Service

You can register the external IP address of the Firebox® X Edge with the dynamic Domain Name Server (DNS) service DynDNS.org. A dynamic DNS service makes sure that the IP address attached to your domain name changes when your ISP gives you a new IP address. For more information, click **Information about Dynamic DNS available here**.

You can also see these WatchGuard FAQs:

What is Dynamic DNS?

How do I set up Dynamic DNS?

https://www.watchguard.com/support/AdvancedFaqs/sogen_main.asp

After you click this link, log into your LiveSecurity Service account to see the FAQ.

NOTE
WatchGuard is not affiliated with DynDNS.org.

---

1   Create a dynamic DNS account.
    For more information, see the Technical Support FAQ "How do I set up Dynamic DNS?

1   To connect to the System Status page, type the IP address of the trusted network in the browser.
    The default IP address is: https://192.168.111.1

2   From the navigation bar, select **Network > Dynamic DNS**.
    The Dynamic DNS client page appears.

Network
Dynamic DNS client
Information about Dynamic DNS available here

☐ Enable Dynamic DNS client
Domain [   ]
Name [   ]
Password [   ]
System [dyndns ▼]
Options [   ]

[Submit]   [Reset]

3   Select the **Enable Dynamic DNS client** check box.

4   Type the **Domain**, **Name**, and **Password** in the related fields.

NOTE
The Firebox gets the IP address of members.dyndns.org when it connects to the time server.

---

5   System???

6   Options???

7   Click **Submit**.

Enabling the WAN Failover Option

The WAN Failover option adds redundant support for the external interface. With this option, the Firebox® X Edge starts a connection through the WAN2 port when the primary external interface (WAN1) can not send traffic. Companies use this option if they must have a constant connection. You must get a second Internet connection to use this option.

It is not necessary to configure new services to use this option. The failover interface uses the same services and network properties as the external interface.

The Firebox uses two methods to find out if the external interface is functional:

• The status of the link to the nearest router

• A ping command to a specified location

The Firebox pings the default gateway or a computer specified by the administrator. If there is no reply, the Firebox changes to the secondary external network interface (WAN2).

When you enable the WAN Failover, the Firebox does the following:

• If the WAN1 interface connection stops, the Firebox starts to use WAN2 interface.

• If the WAN2 interface connection stops, the Firebox starts to use the WAN1 interface.

• If the WAN1 interface and the WAN2 interface stop, the Firebox tries the 2 interfaces until it makes a connection.

When the WAN2 is in use, the Firebox does not switch back to the WAN1 port unless PPPoE is used to assign IP addresses. After the Firebox switches to the WAN2 port, the administrator must change the configuration back to the WAN1 port when the connection is restored.

If you use PPPoE, you can set an inactivity timeout that disables inactive TCP connections during periods of inactivity. See "If your ISP uses PPPoE" on page 48 for PPPoE configuration information. If your external connection fails, the WAN2 port connection is started and used. The WAN2 port is used until the TCP connection becomes inactive (timeout). When the traffic continues, the Firebox connects

through the WAN1 port first. If a connection is made, the WAN1port is used. If the WAN1 port is not available, the Firebox connects through the WAN2 port.

To configure the WAN failover network:

1   Connect one end of a straight through Ethernet cable to the WAN2 interface. Connect the other end to the source of the secondary external network connection. This connection can be a cable modem or a hub.

2   To connect to the System Status page, type the IP address of the trusted network in the browser.
    The default IP address is: https://192.168.111.1

3   From the navigation bar, select **Network > WAN Failover.**
    The WAN Failover page appears.

4   Select the **Enable failover using the Ethernet (WAN2) interface** check box.

5   From the drop-down list, select the interface for the feature: Ethernet or modem (see the next section for additional information on using a modem).

6   Type the IP addresses of the hosts to ping for WAN1 and WAN2 interfaces in the applicable fields.

7   Type the number of seconds between pings and the number of seconds to wait for a reply in the applicable fields.

8   Type the limit number of pings before timeout in the applicable field.

9   Click **Submit**.

Enabling External Modem Failover

Using the Firebox X Edge, you can specify that upon failover the Edge can contact a remote secondary host for routing traffic by way of a modem. For a list of the types of modem supported, see [FAQ?]

1   From the drop-down list on the WAN Failover page, select **Modem (serial port)**.

2   Under **Dial Up Account Settings**, use the drop-down list to select your ISP. The following ISPs are supported: Standard PPP, AOL, AT&T Worldnet, CompuServe 4.0, EarthLink, MSN, and Qwest.

3   Type the telephone number of your ISP. Optionally, you can also type an alternate telephone number.

4   Type the account name used by your ISP for your modem.

5   (Optional) If you use the login to your account with a domain name (such as aol.com), enter it in **Account Domain**.

6   Enter the account password.

7   If you want to enable automatically restoring lost connections, select the corresponding checkbox.

8   If you want to enable modem and PPP debug trace, select the corresponding checkbox.

Modem (serial port) Configuration

| Account | DNS | Dial Up |

Dial Up Account Settings

Internet Service Provider [MSN ▼]

Telephone number [   ]

Alternate telephone number [   ] [optional]

Account name [   ]

Account domain [   ] [optional]

Account password [   ]

☐ Automatically restore lost connections

☐ Enable modem and PPP debug trace

[Submit] [Reset]

DNS settings

If your server is not using DHCP and doesn't specify the location of the DNS server, you must manually enter IP addresses for your DNS server:

1   Select the **Manually configure DNS server IP addresses** checkbox.

2   In the **Primary DNS Server** text box, enter the IP address of the primary DNS server.

3   (Optional) In the **Secondary DNS Server** text box, enter the IP address of the secondary DNS server.

Modem (serial port) Configuration

| Account | DNS | Dial Up |

DNS Settings

☐ Manually configure DNS server IP addresses

Primary DNS server [   ]

Secondary DNS server [   ] [optional]

[Submit] [Reset]

Dialup settings

1 In the **Dial up timeout** field, enter the number of seconds before timeout if your modem doesn't connect.

2 In the **Redial attempts** field, enter the number of attempts made if your modem doesn't connect

3 In the **Inactivity timeout** field, enter the number of seconds before timeout if no traffic passes through the modem.

4 In the **Speaker volume** field, set your modem speaker's volume to off, low, medium, or high.

Modem (serial port) Configuration

Account	DNS	Dial Up

Dialing Options

Dial up time-out [0] (minutes)

Redial attempts [0]

Inactivity Timeout [0] (minutes)

Speaker volume [Off ▼]

[Submit] [Reset]

CHAPTER 5   Setting up the Firebox X Edge Wireless

The Firebox X Edge Wireless protects the computers that are connected to your network. The Firebox X Edge Wireless also protects network wireless connections. This chapter shows how to install the Firebox X Edge Wireless and set up the wireless network.

WatchGuard is concerned about the security of your network so the wireless feature of the Firebox X Edge Wireless is disabled until you are ready to use it. Activate the wireless feature when you configure the security of the wireless connections.

To install the Firebox X Edge Wireless:

• Identify and record your TCP/IP settings

• Disable the HTTP proxy setting of your Web browser

• Activate DHCP on your computer

• Make the physical connections between the Firebox X Edge Wireless and your network

• Attach the two antennae to the Firebox X Edge Wireless

• Install the Firebox X Edge Wireless in a location more than 20 centimeters from all persons. Put the Firebox X Edge Wireless in a location away from all other antennae or transmitters.

To set up the wireless network:

• Configure the wireless network

- Configure the Wireless Access Point (WAP)
- Configure the wireless card on your computer

How Wireless Networking Works

Wireless networking uses radio-frequency signals to communicate with computers and the Firebox X Edge Wireless. The Firebox X Edge Wireless complies with 802.11b and 802.11g standards defined by the Institute of Electrical and Electronics Engineers (IEEE).

You must protect a wireless network from unauthorized access. Without this protection, unauthorized users compromise the security of your network or make use of your Internet connection.

You increase the security of your corporate network by requiring users to authenticate as MUVPN clients. A VPN creates a secure IPSec tunnel from the wireless computer to the Firebox X Edge Wireless. Another way to increase security is to separate the trusted network from the optional network.

Connecting to the Firebox X Edge Wireless

The Firebox X Edge Wireless protects all the computers that connect to your network through the Ethernet ports and wireless connections of the Firebox. This section shows how to connect computers to the Firebox X Edge Wireless using Ethernet cables.

The Firebox X Edge Wireless protects one computer or all the computers on a network. The Firebox X Edge Wireless also operates as a hub to connect other computers.

To set up a wireless network, you connect a computer to the Firebox X Edge Wireless with an Ethernet cable. The computer (the management station) that is connected through an Ethernet cable is used to configure the wireless network.

Cabling the Firebox X Edge Wireless for one to seven devices

A maximum of seven computers, printers, scanners or other devices can connect directly to the Firebox X Edge Wireless. These connections use the seven Ethernet ports (labeled 0-6). There are also two WAN ports (WAN1 and WAN2) you use to create dual ISP connections that provide uninterrupted connectivity. To connect a maxi-

mum of seven devices, use the Firebox X Edge Wireless as a network hub.

1   Shut down your computer.

2   If you connect to the Internet through a DSL modem or cable modem, disconnect the power supply to this device.

3   Disconnect the Ethernet cable that connects your DSL modem, cable modem or other Internet connection to your computer. Connect this cable to the WAN port on the Firebox X Edge Wireless.
    The Firebox X Edge Wireless is connected directly to the modem or other Internet connection.

4   Connect one end of the straight-through Ethernet cable supplied with your Firebox X Edge Wireless to one of the seven numbered Ethernet ports (labeled 0-6) on the Firebox X Edge Wireless. Connect the other end to the Ethernet port of your computer.
    The Firebox X Edge Wireless is connected to the Internet and your computer.

5   If you connect to the Internet through a DSL modem or cable modem, reconnect the power supply to this device. The indicator lights flash and then stop. The modem is available for use.

6   Attach the AC adapter to the Firebox X Edge Wireless. Connect the AC adapter to a power source.

7   Restart the computer.

See "Configuring the External Network" on page 46 and "Configuring the Trusted Network" on page 50 for special configurations.

Cabling the Firebox X Edge Wireless for more than seven devices

Although the Firebox X Edge Wireless has only seven Ethernet ports (labeled 0-6), you can connect more than seven devices. Use one or more network hubs to make more connections.

The base model Firebox X Edge Wireless includes a ten-seat license. This license allows a maximum of ten devices on the trusted network to connect to the Internet at the same time. There can be more than ten devices on the trusted network, but the Firebox X Edge Wireless allows only ten Internet connections. A seat is in use when

a devices connects to the Internet and is free when the connection ends. License upgrades are available from the WatchGuard Web site:

http://www.watchguard.com/sales/buyonline.asp

To connect more than seven devices to the Firebox X Edge Wireless, you need:

- An Ethernet hub
- A straight-through Ethernet cable, with RJ-45 connectors, for each computer
- A straight-through Ethernet cable to connect each hub to the Firebox X Edge Wireless.

To connect more than seven devices to the Firebox X Edge:

1   Shut down your computer. If you connect to the Internet through a DSL modem or cable modem, disconnect the power supply from this device.

2   Disconnect the Ethernet cable that runs from your DSL modem, cable modem, or other Internet connection to your computer. Connect the Ethernet cable to the WAN port on the Firebox X Edge Wireless.
    The Firebox X Edge Wireless is connected directly to the modem or other Internet connection.

3   Connect one end of the straight-through Ethernet cable supplied with your Firebox X Edge Wireless to one of the seven numbered Ethernet ports (labeled 0-6) on the Firebox X Edge Wireless. Connect the other end to the uplink port of the Ethernet hub.
    The Firebox X Edge Wireless is connected to the Internet and your Ethernet hub.

4   Connect an Ethernet cable between each of the computers and an uplink port on the Ethernet hub.

5   If you connect to the Internet through a DSL modem or cable modem, reconnect the power supply to this device. The indicator lights flash and then stop. The modem is available for use.

6   Attach the AC adapter to the Firebox X Edge Wireless. Connect the AC adapter to a power supply.

7   Restart your computer.

Using the Wireless Network Wizard

The Wireless Network Wizard is a tool that you use to automatically configure your wireless network.

Setting up the Wireless Access Point

WatchGuard is concerned about the security of your network so the wireless feature of the Firebox X Edge Wireless is disabed until you are ready to use it. Activate the wireless feature when you configure the security of the wireless connections.

1   Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge Wireless.
    The default IP address is: https://192.168.111.1

1   From the navigation bar, select
    Network > Wireless (802.11g).
    The Wireless Network Configuration page appears.

2   From the **Encryption** drop-down list, select **Disabled**.

3   From the **Authentication** drop-down list, select **Open System**.

4   Record the number that appears in the SSID text box of the Basic Settings for later use.
    The SSID (Service Set Identifier) is the identification number of the wireless device. The SSID is used to create the wireless connection. The default SSID is the 5-digit serial number for your Firebox X Edge Wireless.

5   Click **Submit**.

Configuring the Wireless Card on Your Computer

These instructions are for the Windows XP operating system. To see installation instructions for other operating systems, go to:

http://www.watchguard.com/support/sohoresources/

1   Select **Start > Settings > Control Panel > Network Connections**.
    The Network Connections dialog box appears.

2   Double-click **Wireless Network Connection**.
    The Wireless Network Connection dialog box appears.

3   Select the **Wireless Networks** tab

4   In the **Preferred networks** section, click **Add**.
     The Wireless Network Properties dialog box appears.

5   Type the **SSID** in the **Network Name (SSID)** text box. This is the
     same number that you recorded from the Wireless Network
     Configuration page.

6   Click **OK** to close the **Wireless Network Properties** dialog box.

7   Click **Refresh**.
     All available wireless connections are shown in the Available Networks
     text box. Select the SSID of the computer that you want to configure.

8   Click **OK** to enable the wireless connection.
     The wireless network connection shows that your wireless network is
     active.

9   Configure the wireless computer to use DHCP. For additional
     information about how to configure DHCP, see "Setting your
     computer to use DHCP" on page 20.
     The Windows operating system looks for the wireless connection. If more
     than one wireless network is discovered, a dialog box appears with a list
     of all wireless devices in the area. Select the computer to configure the
     Firebox X Edge Wireless.

The Firebox X Edge Wireless is configured to protect the wired and
wireless computers that are attached to it from security hazards.

Wireless Security Options

The Firebox X Edge provides many options from which to choose in
securing your wireless network.

Two of the most important choices are the security settings:

•   What type of authentication to use

•   The type of encryption to implement

The Firebox X Edge uses two industry-standard security protocols
that provide you with secure wireless protection. They are Wired
Equivalent Privacy (WEP), specified by the IEEE standard 802.11b
and Wi-Fi Protected Access (WPA) supporting theIEEE standard
802.11g. WPA and WEP provide a Wireless Local Area Network
(WLAN) with a level of security and privacy comparable to a wired
Local Area Network (LAN).

A wired LAN is normally protected by measures such as login credentials, which are only effective for a controlled physical environment. Because the radio transmissions of a WLAN are not bound by the walls containing the network, these measures are insufficient for a wireless network. WPA and WEP encrypt the transmissions over the WLAN to provide physical security for the wireless connections between the computers and the access points. In addition, you must use other LAN security mechanisms such as password protection, VPNs, and authentication to ensure privacy.

Follow these instructions to configure the Firebox X Edge Wireless:

1   Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge Wireless:
    The default IP address is: https://192.168.111.1

2   From the navigation bar, select **Network => Wireless Configuration**.
    The Wireless Configuration page appears.

Changing basic settings

The SSID (Service Set Identifier) is the workgroup name of your Wireless Network. You must configure the wireless network card in your computer to have the same SSID in order to communicate with the Firebox X Edge Wireless.

──────────────────── **NOTE** ────────────────────
When you complete the wireless configuration you need to restart the Firebox X Edge wireless.
──

Network assignment offers three choices:

•   None (disable wireless)

•   Bridge to trusted network

•   Bridge to optional network

Select the option that meets your needs.

To change the SSID of the Firebox X Edge Wireless:

•   Type a new identification number in the **SSID** field.
    The default SSID is the 5-digit identification code from the serial number of the Firebox X Edge Wireless. The first four digits of the serial number are the product code and are not used in the SSID. The next five digits of the serial number are the identification code. The remaining characters of the serial number are not used. The maximum length of the SSID is 20 characters.

To change the channel:

• Select a value from the **Channel** drop-down list.

There are four options to choose from in order to set the proper operating region: North America, Europe, France, and Japan. It is very important that you select the proper region because this setting applies to the certification requirements of your region. To configure the operating region select an option from the Operating Region drop-down list.

Configuring security

Select the Authentication mode you want to use for your wireless network connection.

The options are Open System, Shared Key, and Both.

Open System
This option does not support shared keys. If you disable encryption, this is the only option.

Shared Key
This option supports shared keys. If you enabled WPA, this option is enabled.

WPA-PSK
This option activates preshared-keys.

1 From the **Encryption** drop-down list, select the level of encryption for your wireless connections.
The options are Disabled, 64/128 bit WEP, and WPA-PSK.

Disabled
The default setting is Disabled. Use this option for the initial connection. Your wireless connection is not encrypted when Disabled is selected.

64/128 bit WEP or WPA-PSK
After you complete the initial connection between your wireless computer and Firebox X Edge Wireless, you can change the Encryption setting to add WPA-PSK.

2 If you have selected WPA encryption, type a hexadecimal number in the **Key** text boxes.
You can enter up to four keys that the wireless network will use for connections. If you have selected 64 bit WEP, the key can be up to 10 characters. If you have selected 128 bit WEP, the key can be up to 26 characters.

3   If you have typed more than one key, select the key you want to use as the default key from the **Default Key** drop-down list.

Configuring advanced settings

You can configure how the Firebox X Edge Wireless communicates with your wireless computer.

If you want the Firebox X Edge Wireless to broadcast the SSID in the beacon frames, select the Broadcast SSID in AP Beacon Frames checkbox.

The beacon rate is the interval at which the Firebox X Edge Wireless broadcasts a beacon frame to identify itself to wireless computers.

To restrict access to the Firebox X Edge Wireless by the computer hardware address:

1   Select the **Restrict Access by Hardware Address** checkbox.

2   Click **Edit**.
The Allowed Hardware Addresses page appears.

3   Type the MAC Address of the computer that are allowed to connect to the Firebox X Edge Wireless in the applicable field.

4   Click **Add** and then **Submit**.

Wireless computers send requests to determine whether there are any wireless access points to which they can connect. To configure the the Firebox X Edge Wireless to respond to these requests select the Respond to SSID Query Requests checkbox.

Logging authentication events

An authentication event occurs each time a wireless computer attempts to connect to the Firebox X Edge Wireless. If you want the Firebox X Edge Wireless to log authentication events, select the Log Authentication Events checkbox.

To change the fragmentation threshold type a value in the **Fragmentation Threshold** field. The values are 256 through 4096.

Configuring the wireless mode

To configure the operating mode, select an option from the **Wireless Mode** drop-down list. There are three wireless modes from which to select:

802.11g only

This is the default mode, which allows a computer with a wireless network card to access the Firebox X Edge Wireless.

802.11g and 802.11b
This mode allows Firebox X Edge Wireless to connect with wireless devices using both wireless protocols

802.11b only
This mode allows the Firebox X Edge Wireless to connect to devices using this wireless protocol.

Configuring Static Routes

To send the specified packets to different segments of the trusted network connected through a router or switch, configure static routes.

Follow these instructions to configure static routes:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge Wireless:
   The default IP address is: http://192.168.111.1

2 From the navigation bar on the left side, select
   Network > Routes.
   The Routes page appears.

3 Click **Add**.
   The Add Route page appears.

4 From the **Type** drop-down list, select either **Host** or **Network**.

5 Type the IP address and the gateway of the route in the applicable fields.
   The gateway of the route is the local interface of the router.

6 Click **Submit**.

To remove a route, select the route and click **Remove**.

CHAPTER 6   Configuring Firewall Settings

The Firebox X Edge uses firewall properties to control the flow of traffic between the trusted interface and external interfaces. The firewall properties you use show how much risk you can accept.

Configuring Incoming and Outgoing Policies

Your network receives incoming traffic and sends outgoing traffic. Traffic that does not start in your network is incoming traffic. Traffic that starts in your network is outgoing traffic.

The default configuration of the Firebox X Edge prevents the flow of traffic from the external interface to the trusted interface. You add Firebox policies to identify the traffic to transmit between the external and trusted interfaces.

A Firebox policy is one or more rules that together monitor and control traffic. These rules set the firewall actions:

- Allow means to permit a data stream or connection through the Firebox.
- Deny means to stop a data stream or connection from passing through the Firebox, but a response is sent to the source.

To operate a Web server behind the Firebox X Edge, configure the HTTP policy to let incoming traffic flow to the IP address of the Web

server (the internal computer that will receive the requests for Web pages).

You must be careful when you add policies because when you add a policy, you open your Edge to more traffic. When you do this, you increase your risk. Make sure that you compare the value of added access to the security risk.

When you add a policy, you identify the source and destination IP addresses, and set the policy properties.

Standard policies

The Firebox X Edge has standard policies you can use to control the flow of traffic. You can use the procedure below to configure the properties of a standard policy.

1   Type the IP address of the trusted network in your browser window to connect to the System Status page.
    The default IP address is: https://192.168.111.1

2   From the navigation bar, select **Firewall > Incoming** or **Outgoing**.
    The Filter Traffic page appears.

Firewall
Filter Incoming Traffic

Warning:
• Firebox X Edge HTTP service is exposed to the External Network by service: "HTTPS"

Common Services

Filter		Service	Service Host
No Rule		CU-SeeMe	0.0.0.0
No Rule		DNS	0.0.0.0
No Rule		FTP	0.0.0.0
No Rule		HTTP	0.0.0.0
Allow		HTTPS	192.168.111.1
No Rule		ILS	0.0.0.0
No Rule		IPSec	0.0.0.0
No Rule		NetMeeting	0.0.0.0

3   Find a standard policy, such as FTP, Web, or Telnet. From the drop-down list adjacent to the Policy (Service) name, click **Allow** or **Deny**. Repeat to add more policies.

4   For incoming policies, enter the IP address of the service host.

5   Click **Submit**.

Adding a custom policy using the wizard

You can add a custom policy using a TCP port, a UDP port, or a protocol.

1   From the Navigation Bar, click **Wizards**.

2   Next to **Define a custom service...** click **Go**.

3   Obey the on-screen instructions.

The Traffic Filter Wizard includes the following steps:

Step 1: Welcome
The first screen describes what the wizard does and the information you need before running it.

Step 2: Basic Filter Definition
On the next screen, you specify basic information such as the filter name and whether it is appied to incoming or outgoing traffic.

Step 3: Protocols and Ports
Next, you specify the ports you want to assign to this traffic filter.

Step 4: Source Hosts
On the next screen, you identify the IP addresses of the source hosts to which this traffic filter will apply.

Step 5: Destination Hosts
In this step, you identify the IP addresses of the destination hosts to which this traffic filter will apply.

Optional: Destination "service" host
This step appears if you have configured an incoming service to allow traffic from the enternal network to pass through to the trusted network. A local host on the trusted network must be specified as the destination for all traffic matching this filter. This host is referred to as a "service host" because it is generally used

to expose a service such as HTTP (a Web server) to the external network.

Step 6: Summary

The wizard's last screen displays a summary of the settings you have made using the wizard.

Adding a custom policy

You can add a custom policy without using the wizard.

1. In your Web browser, type the IP address of the trusted interface to show the System Status page.
   The default IP address is: https//192.168.111.1

2. On the Filter Traffic page, click **Add Service**.
   The Custom Service page appears.

3. In the Service Name text box, type the name for your policy.

4. From the Protocol drop-down list, click **TCP Port**, **UDP Port**, or **Protocol**.

5   In the text box adjacent to the Protocol drop-down list, type a
    port number or protocol number. To use a range of ports, type a
    port number in the second text box.

──────────────── **NOTE** ────────────────
If you use an IP protocol, do not type a port number. Some of
the IP protocol numbers you can use include:

6   Click **Add**.

The following steps determine how the service is filtered.

7   From the **Incoming Filter** and **Outgoing Filter** drop-down lists,
    click Allow or Deny.

8   From the drop-down list at the bottom of the page, click **Host
    IP Address**, **Network IP Address**, or **Host Range**.

9   In the address text boxes, type the host or network IP address,
    or type the IP addresses that identify range of hosts.

10 Click **Add**.
    Repeat the last three steps until all of the address information for this
    custom service is set.

11 Click **Submit**.

Adding a Policy for the Optional Interface

You can also add policies that monitor and control traffic between
the trusted and optional interfaces:

1   In your Web browser, type the IP address of the trusted interface
    to show the System Status page of the Firebox X Edge.
    The default IP address is: https://192.168.111.1

2   From the navigation bar, click **Firewall** >**Optional**.
    The Filter Outgoing Traffic to Optional Network page appears.

3   From the **Filter** drop-down list, click **Allow**, **Deny** or **No Rule**.

4   Click **Submit**.

Select the **Disable traffic filters** checkbox to allow all incoming and
outgoing traffic between the trusted and optional interfaces.

Firewall
Filter Outgoing Traffic to Optional Network

☐ Disable traffic filters

*Disabling traffic filters will **allow all traffic** in both directions between between the Trusted Network and the Optional Network.*

Filter		Service
No Rule ▼	🖳	DNS
Allow ▼	▫	FTP
No Rule ▼	🌐	HTTP
No Rule ▼	🖳	HTTPS
Deny ▼	POP3	POP3
No Rule ▼	▣	SMTP
Allow ▼	◀	Outgoing

Submit   Reset

Blocking External Sites

The Blocked Sites feature helps prevent unwanted traffic from hostile sites. When you identify a hacker, you can stop all connections that hacker tries to make. When hackers try to connect to your network, the Edge records data about the hacker. You can examine the data to identify attacks.

A blocked site is an external IP address that is blocked from connecting to computers behind the Edge.

The default configuration of the Firebox X Edge:

• Transmits all packets from the trusted interface to the external interface

• Does not transmit all packets from the external network to the trusted network

You can change the configuration to prevent access to specified Internet locations. To add a location to the Blocked Sites list:

1 From the navigation bar, click **Firewall** >**Blocked Sites.**
   The Blocked Sites page appears.

2   From the drop-down list, click **Host IP Address**, **Network IP Address**, or **Host Range.**

3   In the text box, type a host IP address, a network IP address, or a range of host IP addresses.

4   Click **Add**.
     The address information appears in the Blocked Sites list.

5   Click **Submit**.

Configuring Firewall Options

The sections before this one tell how to create a policy that allows, or denies, a specified type of traffic. You use the Firewall Options page to add non-policy security measures.

1   Connect to the System Status page of the Firebox X Edge.
     The default IP address is: https://192.168.111.1

2   From the navigation bar, click **Firewall > Options.**
     The Firewall Options page appears.

```
Firewall
Firewall Options


☐ Do not respond to PING requests received on External Network.
☐ Do not respond to PING requests received on Trusted Network.
☐ Do not allow FTP access to Trusted Network interface.
☐ Disable SOCKS proxy.
☐ Log All Allowed Outbound Access.
☐ Enable override MAC address for the External Network.
     External Network override MAC address    [            ]
☐ Enable override MAC address for the Failover Network.
     Failover Network override MAC address    [            ]

  Submit    Reset
```

Responding to ping requests

You can configure the Firebox X Edge to deny pings.

1   Select the **Do not respond to PING requests received on
    External Network** checkbox or the **Do not respond to PING
    requests received on Trusted Network** checkbox.

2   Click **Submit**.

Denying FTP access to the trusted network interface

You can configure the Firebox X Edge to stop FTP traffic from the
trusted interface or external interface.

1   Select the **Do not allow FTP access to Trusted Network**
    checkbox.

2   Click **Submit**.

──────────────────── **NOTE** ────────────────────
You must clear the Do not allow FTP access to Trusted Network
checkbox or the Software Update Installer cannot move firmware
files to the Firebox X Edge.
───

SOCKS implementation for the Firebox X Edge

The Firebox X Edge can operate as a SOCKS network proxy server.
Software that uses more than one socket connection and uses the
SOCKS version 5 protocol can send traffic through the Edge. SOCKS
gives you secure, two-way communication between a computer on
the external network and a computer on the trusted network. To use

a SOCKS-compatible program, configure the program with the necessary information about the Firebox X Edge.

The Firebox X Edge uses SOCKS version 5. The Firebox X Edge users do not authenticate before using the Edge configuration pages.

Your Firebox X Edge does not speak with software that finds only DNS (domain name server) names. Configure the SOCKS-compatible software to connect to IP addresses and not connect to domain names.

Software that uses SOCKS and can operate with Firebox X Edge includes ICQ, IRC, and AOL Messenger.

───────────────── **NOTE** ─────────────────

If software that uses SOCKS operates on a computer put on the trusted network, then all users on the trusted network can use the SOCKS proxy. To kill this risk, disable the SOCKS proxy on your Firebox X Edge.

Configuring your SOCKS application

Configure the software using SOCKS on computers put on the trusted network to speak with a computer on the external network. When you configure that software, use the recommended properties from that software documentation.

───────────────── **NOTE** ─────────────────

The Firebox X Edge uses port 1080 to speak to computers with software using SOCKS. Make sure that port 1080 is open and not used by other software on the computer.

1 If you get to identify a version, select SOCKS version 5.

2 Select port 1080.

3 Set the SOCKS proxy to the URL (uniform resorce locator) or IP address of the Firebox X Edge. The default IP address is: https://192.168.111.1.

Disabling SOCKS on the Edge

When the software using SOCKS stops, port 1080 stays open. To kill this security risk, close the port when the software stops.

1 On the Firewall Options page, select the **Disable SOCKS proxy** checkbox.
   The SOCKS Proxy is disabled.

2 Click **Submit**.

To use the SOCKS-compatible application:

1   Clear the **Disable SOCKS proxy** checkbox.
    The SOCKS proxy is enabled.

2   Click **Submit**.

Logging all allowed outbound traffic

If you use the standard property settings, the Firebox X Edge records only unusual events. When traffic is denied, the Edge records the information in the log file. You can configure the Edge to record information about all the outgoing traffic in the log file.

NOTE

Recording all outgoing traffic creates a large number of log records. WatchGuard recommends that you record all the outgoing traffic only as a problem-solving aid.

To record all outgoing traffic:

1   Select the **Log All Allowed Outbound Access** checkbox.

2   Click **Submit**.

Stop using the current MAC address

Your ISP can register the MAC address of your computer and accept attempts to connect only from that MAC address. You can change this property to use the MAC address that connected to the ISP on this line in the past. The MAC address must obey these conditions:

•   The MAC address must use 12 hexadecimal characters (hhhhhhhhhhhh) with a value between 0 and 9 or between "a" and "f".

•   The MAC address must operate with:
    -   One or more addresses on the external network
    -   The MAC address of the trusted network for the Firebox X Edge
    -   The MAC address of the optional network for the The Firebox X Edge

•   The MAC address cannot be set to 000000000000

•   The MAC address cannot be set to ffffffffffff (0012340ABCDE)

To stop using the current MAC address:

1   Select the **Enable override MAC address for the External Network** checkbox, or select the **Enable override MAC address for the Failover Network** checkbox.
    You can select the checkboxes together.

2   In the **External network override AC address** or **Failover network override AC address** text box, type the new MAC address for the Firebox X Edge external or failover network.

3   Click **Submit**.

───────────────── **NOTE** ─────────────────
If the **MAC address for the external network** field is cleared and the Firebox X Edge is restarted, the Firebox X Edge uses the standard MAC address for the external network.
──

To stop MAC address problems, the Firebox X Edge finds the current MAC address at regular intervals. If the Edge finds a device using the same MAC address, the Firebox changes to the standard MAC address for the external network. Then the Edge restarts.

Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.

Configuring Logging

A log file is a record of all the events that occur on the Firebox® X Edge. An *event* is any single activity, such as the denial of a packet entering the Firebox. *Logging* records and saves information about these events.

Log records give a list of possible security problems. An event log is an important part of a network security policy. A sequence of denied packets can show a pattern of inappropriate network activity.

NOTE

The Firebox X Edge log is cleared if the power supply is disconnected or rebooted from the Edge. The information is not cleared if an external Syslog or WSEP logging host is configured.

Viewing Log Messages

The Firebox X Edge records a maximum of 150 log messages. New information appears at top of the file. When new information enters a full message file, it erases the oldest log message.

The log messages include the time synchronizations between the Firebox X Edge and the WatchGuard Time Server. Packets are cleared because of a packet handling violation, duplicate messages, return error messages, and IPSec messages.

Each log message contains this information:

Time
The time of the event that created the log message.

Category
The category of the message. For example, whether the message came from an IP address or from a configuration file.

Message
The text of the message

This procedure shows how to view the event log:

1   Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
    The default IP address: https://192.168.111.1

2   From the navigation bar, select **Logging**.
    The Logging page appears with the Event Log at the bottom of the page.

Event Log

Time	Category	Message
2004-07-01-02:25:53	MONITOR	Administrator access allowed from 10.168.3.90
2004-07-01-02:25:52	IP	allowed from 10.168.3.90 port 3382 to 192.168.54.54 port 443 TCP SYN (HTTPS)
2004-07-01-02:25:17	MONITOR	Timeout opening connection to log server
2004-07-01-02:25:08	IP	discard from 192.168.54.57 to to 192.168.54.54 ICMP type (3) code (3)(SIP discarded)

Logging to a WatchGuard Security Event Processor Log Host

The WatchGuard Security Event Processor (WSEP) is a program that is available with the WatchGuard System Manager. If you have a Firebox® III or Firebox X, configure the WSEP to accept the log messages from your Firebox X Edge. For instructions on how to configure the WSEP to accept the log messages, see the *WatchGuard System Manager User Guide*. Then follow these instructions to send your event logs to the WSEP.

1   Type the IP address of the trusted network in your browser window.
    The default IP address: https://192.168.111.1

2   From the navigation bar, select **Logging > WSEP Logging.**
The WatchGuard Security Event Processor Logging page appears.

Logging
WatchGuard Security Event Processor Logging

☑ Enable WatchGuard Security Event Processor Logging
Log Host IP Address [192.168.54.57]
Log Encryption Key [●●●●●]
Confirm Key [●●●●●]
Device Name [PT&P]

[Submit] [Reset]

3   The **Enable WatchGuard Security Event Processor Logging** checkbox
should contain a checkmark. If it does not, select it.

4   In the **Log Host IP Address** field, type the IP address of the WSEP server
that is your log host.

5   Type a passphrase in the **Log Encryption Key** field and confirm the
passphrase in the **Confirm Key** field.

6   In the **Device Name** field, type a name for the Firebox X Edge.
This identifier lets the WSEP log host distinguish between different devices
logging to it. If this field is empty, the Firebox X Edge is identified to the WSEP log
host by the IP address of the Firebox's external interface.

7   Click **Submit**.

――――――――――――― **NOTE** ―――――――――――――
Use the same log encryption key used by the WSEP application.
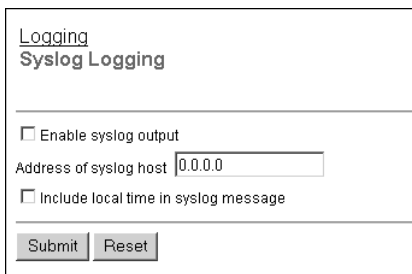
Logging to a Syslog Host

Syslog is a logging interface, developed for UNIX also used by a number of
computer systems. This option sends the Firebox® X Edge log messages to a
Syslog host. If you already maintain a Syslog host, set the Edge to send log
messages to that host.

Configure a Syslog host:

1   Type the IP address of the trusted network in your browser window.
    The default IP address: https://192.168.111.1

2   From the navigation bar, select **Logging > Syslog Logging**.
    The Syslog Logging page appears.

Logging
Syslog Logging

☐ Enable syslog output
Address of syslog host 0.0.0.0
☐ Include local time in syslog message

Submit   Reset

3   Select the **Enable Syslog output** checkbox.

4   Next to **Address of Syslog host**, type the IP address of the computer running Syslog.

5   (Optional) Select the **Include local time in syslog message** checkbox to include the local time in the Syslog messages.

6   Click **Submit**.

──────────────── **NOTE** ────────────────

Because Syslog traffic is not encrypted, Syslog messages that are sent through the Internet decrease the security of the trusted network. Use a VPN tunnel to increase the security of Syslog message traffic. If the Syslog messages travel through a VPN tunnel, the data is encrypted with IPSec technology.

Setting the System Time

For each log record, the Firebox® X Edge records the time from its system clock.

You set the time one of two ways. You synchronize your system using Network TIme Protocol (NTP) or you can set the date and time manually.

Set the system time:

1   Type the IP address of the trusted network in your browser
    window.
    The default IP address: https://192.168.111.1

2   From the navigation bar, select **Logging > System Time**.
    The System Time page appears.

3   ....time zone from the drop-down list.

4   (Optional) Select **Adjust for daylight savings time**.

5   Select the method to set system time.

6   Click **Submit**.

Setting time using NTP

Network Time Protocol (NTP) synchronizes the clocks of computers on a network. For more information on NTP, see http://www.ntp.org.

1   From the System Time page, select **Use NTP to periodically automatically set system time**.

2   Select an NTP server from the list. Or, type the name of a new server and click **Add**. You can add a maximum of 16 NTP servers.

Setting time manually

1   From the System Time page, select **Set date and time manually**.

2   From the drop-down list, specify set the date using input fields or synchonize time with the browser.

3   If you chose to set time using input fields, set the date and time using the calendar and fields provided.

    If you chose to set time by synchronizing, click **Synchronize Now** when you are ready to synchronize.

Configuring WebBlocker

Security is one of the most important reasons to purchase and install a firewall. The Firebox X Edge, when used with the WebBlocker feature, is one of the most secure firewalls available.

All companies face web content threats such as:

Productivity
Recreational Web surfing decreases overall productivity.

Legal Concerns
Employees can sue if they do not have a work environment free of gender and minority harassment. You must take reasonable care to stop offensive Internet content.

Network Threats
An employee can crash your network by logging into the incorrect Web site. Other activity such as recreational surfing and downloading MP3 files divert valuable bandwidth from critical business needs.

Security
Many viruses enter networks through web-based e-mail accounts or through other files downloaded from the Web.

WebBlocker is an option for the WatchGuard® Firebox® X Edge that gives you control over which Web sites are available.

<hr>

NOTE

You must purchase the WebBlocker upgrade to use this feature. For information on activating upgrade options, see "Activating Upgrade Options" on page 161.

<hr>

How WebBlocker Works

WebBlocker uses a database of Web site addresses maintained by SurfControl®.

When a user on your network tries to open a Web site, the Firebox® queries the database. If the Web site is not in the WatchGuard Web-Blocker database or not blocked the page opens. If the site is blocked a notification appears.

Configuring Global WebBlocker Settings

The first WebBlocker page in the Firebox® X Edge Web pages is the WebBlocker Settings page. Use this page to:

- Activate WebBlocker
- Set the full access password
- Set the inactivity timeout
- Make sure that your Web users authenticate

To configure WebBlocker:

1   Type the IP address of the trusted network in your browser window.
    The default IP address: https://192.168.111.1

2   From the navigation bar, select **WebBlocker > Settings.**
    The WebBlocker Settings page appears.

WebBlocker
Settings

☑ Enable WebBlocker
        Full Access Password [********]
        Confirm Password [********]
Inactivity Timeout (minutes) [0]
☐ Require Web users to authenticate

[Submit]

3   Select the **Enable WebBlocker** check box.

4   Type a password in the **Full Access Password** field.
    The full access password gives access all Web sites until the password expires or the browser is closed.

5   Type the same password again in the **Confirm Password** field.

6   Type a number, in minutes, in the **Inactivity Timeout field**.
    The inactivity timeout breaks Internet connections that are inactive for the set number of minutes.

7   To make users authenticate for Internet access, select **Require Web users to authenticate**.

8   Click **Submit**.

Creating WebBlocker Profiles

A WebBlocker profile is a set of restrictions you apply to users on your network. You can create a profile that contains a restriction that limits use for new employees with less than 90 days tenure. Then create a less restrictive profile for users when the initial probationary period is complete.
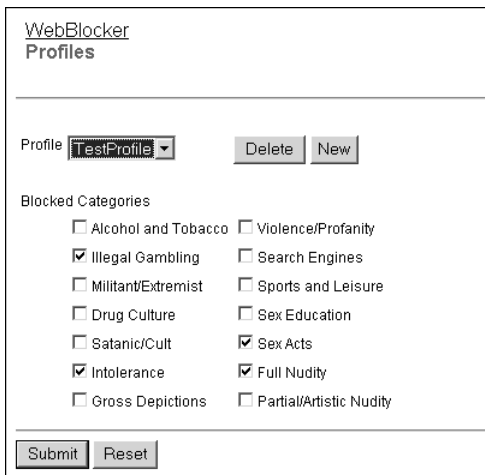
After you define profiles, you can apply them when you set up accounts. This procedure appears in Chapter 10, "Managing the Firebox X Edge."

1   Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox® X Edge.
    The default IP address: https://192.168.111.1

2   From the navigation bar, select **WebBlocker > Profiles**.
    The Profiles page appears.

3   Click **New.**
    The New Profile page appears.

4   In the **Profile Name** field, type a familiar name.
    You use this name to identify the profile during later configuration. For example, give the name "90day" to an employee at your company for less than 90 days.

5   In **Blocked Categories**, click the categories of Web sites you do not want your employees to see.
    For more information on categories, see the next section.

6   Click **Submit**.

To delete a profile, from the WebBlocker Profiles page, select the profile from the **Profile** drop-down list. Click **Delete**.

WebBlocker Categories

The WebBlocker database contains 14 categories.

A Web site is added to a category when the contents of the Web site meet the correct criteria. Web sites that give opinion or educational material about the subject matter of the category are not included. For example, the drugs/drug culture category denies sites that tell how to grow and use marijuana. They do not deny sites with information about the historical use of marijuana.

The categories:

Alcohol/tobacco
Pictures or text that advocate the sale, consumption or production of alcoholic beverages and tobacco products.

Illegal Gambling
Pictures or text advocating materials or activities that may be illegal in any or all jurisdictions. Some examples are illegal business schemes, chain letters, copyright infringement, computer hacking, phreaking (using phone lines without permission), and piracy. Also includes text advocating gambling relating to lotteries, casinos, betting, numbers games, online sports or financial betting, including non-monetary dares.

Militant/extremist
Pictures or text advocating extremely aggressive or combative behavior or advocacy of unlawful political measures. Topic includes groups that advocate violence as a means to achieve their goals. It also includes pages devoted to "how to" information on the making of weapons (for both lawful and unlawful reasons), ammunition, and pyrotechnics.

Drug Culture
Pictures or text advocating the illegal use of drugs for entertainment. This category includes substances that are used for other than their primary purpose to alter the individual's state of mind. This does not include currently illegal drugs legally prescribed for medicinal purposes (such as drugs used to treat glaucoma or cancer).

Satanic/cult

Pictures or text advocating devil worship, an affinity for evil, wickedness, or the advocacy to join a cult. A cult is a closed society that is headed by an individual, loyalty is demanded and leaving is forbidden.

Intolerance

Pictures or text advocating prejudice or discrimination against any race, color, national origin, religion, disability or handicap, gender, or sexual orientation. Any picture or text that elevates one group over another. Also includes intolerant jokes or slurs.

Gross Depictions

Pictures or text describing anyone or anything that is either crudely vulgar, grossly deficient in civility or behavior, or shows scatological impropriety. Topic includes depictions of maiming, bloody figures, and indecent depiction of bodily functions.

Violence/profanity

Pictures or text exposing extreme cruelty or profanity. Cruelty is physical or emotional acts against any animal or person that are primarily intended to hurt or inflict pain. This includes obscene words, phrases, and profanity in audio, text, or pictures.

Search Engines

Search engine sites such as Google.

Sports and Leisure

Pictures or text describing sporting events, sports figures or other entertainment activities.

Sex Education

Pictures or text advocating the proper use of contraceptives. Topic includes sites devoted to the explanation and description of condoms, oral contraceptives, intrauterine appliances, and other types of contraceptives. It also includes discussion sites devoted to conversations with partners about sexually transmitted diseases, pregnancy, and sexual boundaries. Not included in this category are commercial sites selling sexual paraphernalia (topics included under *Sexual Acts*).

Sexual Acts

Pictures or text exposing anyone or anything involved in explicit sexual acts and/or lewd and lascivious behavior. Topic includes

masturbation, copulation, pedophilia, as well as intimacy involving nude or partially nude people in heterosexual, bisexual, lesbian, or homosexual encounters. It also includes phone sex advertisements, dating services, adult personals, and sites devoted to selling pornographic CD-ROMs and videos.

Full Nudity

Pictures exposing any or all portions of human genitalia. Topic does *not* include sites categorized as Partial/Artistic Nudity containing partial nudity of a wholesome nature. It does not include Web sites for publications such as *National Geographic* or *Smithsonian* magazine or sites hosted by museums such as the Guggenheim, the Louvre or the Museum of Modern Art.

Partial/artistic Nudity

Pictures exposing the female breast or full exposure of either male or female buttocks except when exposing genitalia that is handled in the Full Nudity category. Topic does not include swimsuits, including thongs.

For information on how to see whether specific sites are included in the SurfControl database, and for more information on WebBlocker categories, see

https://www.watchguard.com/support/AdvancedFaqs/web_main.asp

- How can I see a list of blocked sites?
- How do different sites map into WebBlocker's 14 categories?

Allowing Certain Sites to Bypass WebBlocker

Some sites are useful even when they are denied by WebBlocker. You can allow these sites regardless of other WebBlocker settings.

For example, employees in your company might need to see Web sites that contain medical information. Some of these sites are forbidden by WebBlocker because they fall into the category of sex education. You override the WebBlocker setting by adding the site to the Allowed Sites list.

This WebBlocker feature is applicable only for outbound Web accesss. You cannot use WebBlocker exceptions to not include an internal host in WebBlocker rules.

1   From the navigation bar, select **WebBlocker > Allowed Sites.**
    The WebBlocker Allowed Sites page appears.
2   From the drop-down list, specify a host IP address, network IP address or host range.
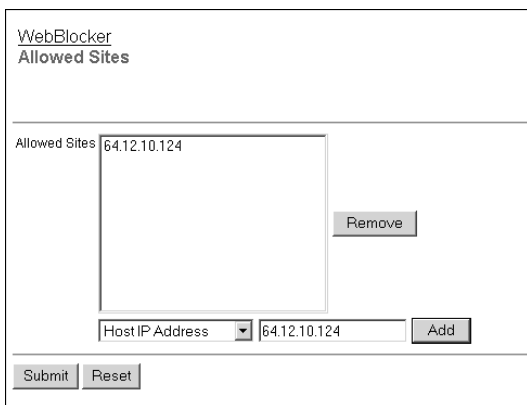
3   Type the host or network IP address of the allowed site. If it is a range, type the start and end point of the range. Click **Add**.
4   Do step 3 again for other allowed sites. When have no more sites to add, click **Submit**.

To remove an item from the list, select the address. Click **Remove**.

Blocking Additional Web Sites

You might not want your users to see certain sites even if Web-Blocker allows them. For example, you may receive a LiveSecurity® Service alert warning that a certain commonly used Web site is dangerous. Using the Denied Sites feature to make sure your employees do not look at this site.

1   From the navigation bar, select **WebBlocker > Denied Sites**.
    The WebBlocker Denied Sites page appears.

2   From the drop-down list, specify a host IP address, network IP address or host range.

WebBlocker
Denied Sites

Denied Sites 64.12.10.127

Remove

Host IP Address ▼ 64.12.10.127 Add

Submit Reset

3   Type the host or network IP address of the denied site. If it is a range, type the start and end point of the range. Click **Add**.

4   Do step 3 for other denied sites. When you have no more sites to add, click **Submit**.
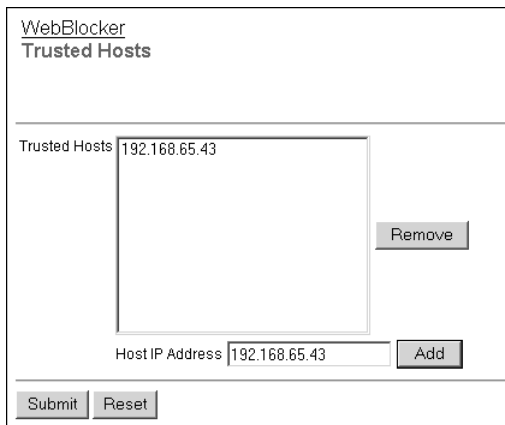
To subtract an item from the list, select the address. Click **Remove**.

Allowing Internal Hosts to Bypass WebBlocker

You can make a list of internal hosts that bypass WebBlocker set-
tings:

1   From the navigation bar, select **WebBlocker > Trusted Hosts.**
    The WebBlocker Trusted Hosts page appears.

```
WebBlocker
Trusted Hosts


Trusted Hosts  [ 192.168.65.43              ]

                              [ Remove ]


        Host IP Address [192.168.65.43]   [ Add ]

  [ Submit ]  [ Reset ]
```

2   In the text box at the bottom of the page, type the host IP
    address of the site to allow. Click **Add.**
3   Do step 3 again for other allowed hosts. When you have no
    more hosts to add, click **Submit.**

To subtract an item from the list, select the address. Click **Remove.**

Configuring Virtual Private Networks

You use a virtual network (VPN) to create secure connections between computers or networks in different locations. The networks and hosts on a VPN can be corporate headquarters, branch offices, remote users, and telecommuters. VPN tunnels are secured, and the identity of the sender and the receiver are authenticated. Data on the tunnel is encrypted. Only the sender and the receiver of the message can read it.

What You Need to Create a VPN

- Two Firebox X Edge devices or one Firebox X Edge and a second device that uses IPSec standards. An example of such a device is a Firebox X. You must enable the VPN option on each device.
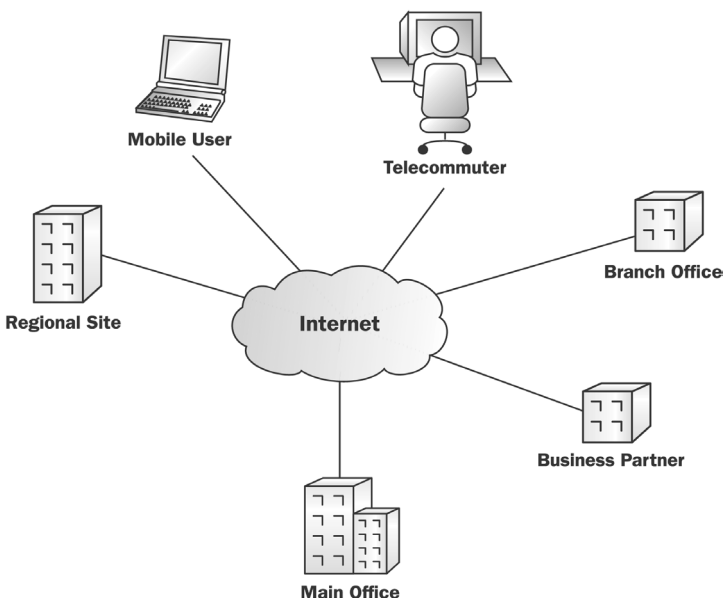
- The static IP address of each Firebox X Edge external interface.
- The network address of the private (trusted) network located behind each Firebox X Edge (the networks that will communicate through the), and their subnet masks. The base trusted IP address of each Firebox X Edge must be static and unique.
- The DNS and WINS server IP addresses, if used.
- The shared key (passphrase) for the tunnel. The same shared key must be used by both devices.
- The same encryption method for each end of the tunnel (DES or 3DES).
- The same authentication method for each end of the tunnel (MD5 or SHA1).

<hr>

NOTE

The trusted networks at each end of the VPN tunnel must have different network addresses.

<hr>

VPN requirements

Before you configure your WatchGuard Firebox X Edge VPN network:

- You can connect a maximum of 10 Firebox X Edge devices together in a star configuration. To configure more VPN tunnels, a WatchGuard Firebox III or Firebox X and WatchGuard VPN Manager is necessary.

- WatchGuard recommends that each VPN device has a static IP address. Configuring a VPN tunnel between devices that use dynamic IP addresses can cause problems. See "Network addressing" on page 5 for more information about dynamic IP addresses. Dynamic IP address problems can be resolved with Dynamic DNS. For Dynamic DNS configuration information, see "Registering with the Dynamic DNS Service" on page 62.

- VPN devices must use the same encryption method, DES or 3DES.

- If you connect two Microsoft Windows NT networks, they must be in the same Microsoft Windows domain, or they must be trusted domains. This is a Microsoft Networking issue, and not a limitation of the Firebox X Edge.

We recommend that you record your Firebox X Edge configuration. Use the Sample VPN Address Information table on the next page to write down this information.

Sample VPN Address Information Table

Item	Description	Assigned By
External IP Address	The IP address that identifies the IPSec-compatible device on the Internet. Site A: 207.168.55.2 Site B: 68.130.44.15	ISP
External Subnet Mask	The bitmask that shows which part of the IP address identifies the local network. For example, a class C address includes 256 addresses and has a netmask of 255.255.255.0.(Only 254 of the IP addresses in that subnet can be assigned to computers.) Site A: 255.255.255.0 Site B: 255.255.255.0	ISP
Local Network Address	An address used to identify a local network. A local network address cannot be used as an external IP address. WatchGuard recommends that you use an address from one of the reserved ranges: 10.0.0.0/8—255.0.0.0 172.16.0.0/12—255.240.0.0 192.168.0.0/16—255.255.0.0 The numbers after the slashes indicate the subnet masks. /24 means that the subnet mask for the trusted network is 255.255.255.0. For more information on entering IP addresses in slash notation, see the FAQ: https://www.watchguard.com/support/advancedfaqs/general_slash.asp Site A: 192.168.111.0/24 Site B: 192.168.222.0/24	You
Shared Secret	The shared secret is a passphrase used by two IPSec-compatible devices to encrypt and decrypt the data that goes through the VPN tunnel. The two devices use the same passphrase. If the devices do not have the same passphrase, they cannot encrypt and decrypt the data correctly. Use a passphrase that contains numbers, symbols, lowercase letters, and uppercase letters for better security. For example, "Gu4c4mo!3" is better than "guacamole". Site A: OurSharedSecret Site B: OurSharedSecret	You

Item	Description	Assigned By
Encryption Method	DES uses 56-bit encryption. 3DES uses 168-bit encryption. The 3DES encryption method is more secure, but slower. The two devices must use the same encryption method. Site A: 3DES Site B: 3DES	You
Authentication	The two devices must use the same authentication method. Site A: MD5 (or SHA1) Site B: MD5 (or SHA1)	You

Using a DVCP server to create your VPN tunnels

Dynamic VPN Configuration Protocol (DVCP) is the WatchGuard protocol that creates IPSec tunnels. The VPN tunnel configurations are saved on the DVCP server. This decreases the work for the administrator.

You can only use a Firebox III or Firebox X model as a DVCP server. You can easily create tunnels on the Firebox X Edge by configuring it as a DVCP client.

There are two kinds of DVCP servers:

• Basic DVCP - All Firebox III and Firebox X models

• VPN Manager - Firebox III 1000 or above, Firebox X700 or above

For more information, see the FAQ:

https://www.watchguard.com/support/advancedFAQs/basicdvcp_whatis.asp
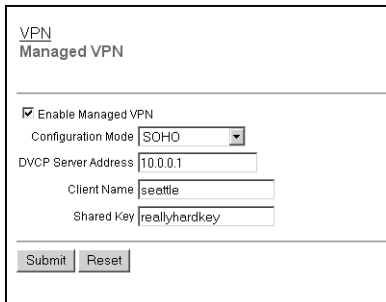
Setting up management for a dynamic Edge device

Use this procedure for a Firebox X Edge device with a dynamic IP address for the external interface.

1   Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1.

2   From the navigation bar, select **VPN > Managed VPN**.
     The Managed VPN page appears.
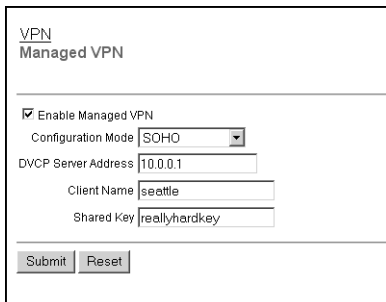
3   Select the **Enable Managed VPN** checkbox.

4   Type the IP address of the DVCP server.

5   Type the client name and the shared key. If you have a Basic
     DVCP server, use the client name. If you have a VPN Manager
     DVCP server, use the host name.

6   Click **Submit**.

Setting up management for a static Edge device

If you use a Basic DVCP server and the Firebox X Edge has a static IP
address, use this procedure:

1   Type the IP address of the trusted network in your browser
     window to connect to the System Status page of the Firebox X
     Edge.
     The default IP address is: https://192.168.111.1.

2   From the navigation bar, select **VPN > Managed VPN**.
     The Managed VPN page appears.

3   Select the **Enable Managed VPN** checkbox.

4   Type the IP address of the DVCP server.

5   Type the client name and the shared key. Use the Client Name
     you entered on the Basic DVCP server.

6   Click **Submit**.

Setting Up Manual VPN Tunnels

You can configure a maximum of 10 tunnels from the Firebox X
Edge to other Firebox X Edge devices. The VPN Manager software
can configure a larger number of Firebox X Edge to Firebox X Edge
tunnels.

To define VPN tunnels to other Firebox X Edge devices:

1   Type the IP address of the trusted network in your browser
     window to connect to the System Status page of the Firebox X
     Edge.
     The default IP address is: https://192.168.111.1.

2   From the navigation bar, select **VPN** > **Manual VPN**.
     The Manual VPN page appears.

3   Click **Add**.
     The Add Gateway page appears.

4   Type the **Name** and **Shared Key** for the VPN tunnel.
   The shared key is a passphrase that the devices use to encrypt and
   decrypt the data on the VPN tunnel. The two devices use the same
   passphrase. If the devices do not have the same passphrase, they cannot
   encrypt and decrypt the data correctly.

Phase 1 settings

Internet Key Exchange (IKE) is a protocol used with VPNs to manage
keys automatically. IKE negotiates keys and changes keys. Phase 1
authenticates the parties and creates a key management security
association to protect tunnel data.

The default settings for Phase 1 are the same for all Firebox X
devices. Many users keep these settings in their default values.

───────────────── **NOTE** ─────────────────
Make sure that the Phase 1 configuration is the same on both
devices.

To change Phase 1 configuration:

1   Select the negotiation mode for Phase 1 from the drop-down list.

    You can use main mode only when both devices have static IP addresses. If one VPN or both devices have IP addresses that are dynamically assigned, you must use aggressive mode.

2   Enter the local ID and remote ID. Select the ID types—**IP Address** or **Domain Name**—from the drop-down lists. Make sure this configuration is the same as the configuration on the remote device.

    -   If you select **Main Mode** and the remote ID type is **IP Address**, this must be the remote gateway's IP address.

    -   If you select **Aggressive Mode** and the remote gateway is static, set the remote ID type to **IP Address**. If the local gateway is static, set the local ID type to **IP Address**. If the remote gateway is dynamic, set the local ID type to **Domain Name**. If the remote gateway is dynamic and uses dynamic DNS, set the remote ID type to **Domain Name** and the remote ID to the DNS name.

3   Select the type of authentication from the **Authentication Algorithm** drop-down list.

    The options are MD5-HMAC (128-bit authentication) or SHA1-HMAC (160-bit authentication).

4   From the **Encryption Algorithm** drop-down list, select the type of encryption.

    The options are DES-CBC or 3DES-CBC.

5   Type the number of kilobytes and the number of hours until the IKE negotiation expires.

6   Select the group numbr from the **Diffie–Hellman Group** drop-down list. WatchGuard supports group 1 and group 2.

    Diffie-Hellman groups securely negotiate secret keys through a public network. Group 2 is more secure than group 1, but requires more processing power and more time.

7   Select the **Generate IKE Keep Alive Messages** checkbox to help detect when the tunnel is down.

    Select this checkbox to send short packets across the tunnel at regular intervals. This helps the two devices to determine that the tunnel still works securely. If the Keep Alive packets get no response after three attempts, the Firebox X Edge does a rekey to start the tunnel again.

━━━━━━━━━━━━━━━ **NOTE** ━━━━━━━━━━━━━━━
The IKE Keep Alive feature is different from the VPN Keep Alive feature described in"VPN Keep Alive," on page 117.

Phase 2 settings

Phase 2 negotiates the data management security association for the tunnel. The tunnel uses this phase to create IPSec tunnels and encapsulate and decapsulate data packets.

You can use the default Phase 2 settings to simplify configuration.

━━━━━━━━━━━━━━━ **NOTE** ━━━━━━━━━━━━━━━
Make sure that the Phase 2 configuration is the same on both devices.

To change the Phase 2 settings:

1   Select the authentication method from the **Authentication Algorithm** drop-down list.

2   Select the encryption algorithm from the **Encryption Algorithm** drop-down list.

3   If you are using Perfect Forward Secrecy, select the **Enable Perfect Forward Secrecy** checkbox.
    This option makes sure that each new key is derived from a new Diffie-Hellman exchange. This option makes the negotiation more secure, but requires more time.

4   Type the number of kilobytes and the number of hours until the IKE negotiation expires.

5   Type the IP address of the local network and the remote network that must use Phase 2 negotiation.
    Network addresses must be entered in "slash" notation (also known as Classless Inter Domain Routing or CIDR notation). For more information on entering IP addresses in slash notation, see the following FAQ: http://www.watchguard.com/support/advancedfaqs/general_slash.asp.

6   Click **Add**.

7   Click **Submit**.

Phase 2 Settings
Authentication Algorithm SHA1-HMAC
Encryption Algorithm 3DES-CBC
☐ Enable Perfect Forward Secrecy
Key expiration in kilobytes 8192
Key expiration in hours 24

The Firebox X Edge will create a tunnel for each remote network defined below. In order to interoperate properly, the remote peer must be configured the same way.

Local Network	Remote Network

Remove

Local Network 0.0.0.0/0
Remote Network 0.0.0.0/0   Add

Submit   Reset
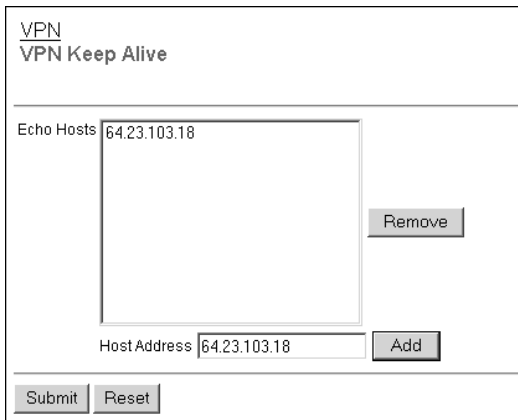
VPN Keep Alive

To keep the VPN tunnel open when there is no communication across it, you can use the IP address of a computer at the other end of the tunnel. The Firebox® X Edge will send a ping once a minute to the specified host. Use the IP address of a host that is always up, and that responds to ping messages. You can enter the trusted interface IP address of the Firebox X Edge, or the trusted interface IP address of a Firebox III or Firebox X that is at the other end of the tunnel. You can use multiple IP addresses so the Firebox X Edge can ping multiple hosts across different tunnels.

1   Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1

2   From the navigation bar, select **VPN > Keep Alive**.
     The VPN Keep Alive page appears.

3   Type the IP address of an echo host. Click **Add**.

4   Click **Submit**.

Viewing VPN Statistics

You can monitor VPN traffic and troubleshoot the VPN configura-
tion. with the VPN Statistics page.

To view the VPN Statistics page:

1   Type the IP address of the trusted network in your browser
     window to connect to the System Status page of the Firebox X
     Edge.
     The default IP address is: https://192.168.111.1

2   From the navigation bar, select **VPN > VPN Statistics**.
     The VPN Statistics page appears.

Frequently Asked Questions

Why do I need a static external address?

To make a VPN connection, each device must know the IP address
of the other device. If the address for a device is dynamic, the IP
address can change. if the IP address changes, connections between
the devices cannot be made.

This issue can be resolved with Dynamic DNS. For information, see "Registering with the Dynamic DNS Service" on page 62.

How do I get a static external IP address?

You get the external IP address for your computer or network from your ISP or an administrator. Many ISPs use dynamic IP addresses to make their networks easier to configure and easier to use with many users. Most ISPs can give you a static IP address as an option.

How do I troubleshoot the connection?

If you can ping the trusted interface of the remote Firebox X Edge and the computers on the remote network, the VPN tunnel is up. The configuration of the network software or the applications are possible causes of other problems.

Why is ping not working?

If you cannot ping the local interface address of the remote Firebox X Edge, follow these steps:

1   Ping the external address of the remote Firebox X Edge.

For example, at Site A, ping 68.130.44.15 (Site B). If the ping packet does not come back, make sure the external network settings of Site B are correct. (Site B must be configured to respond to ping requests on that interface.) If the settings are correct, make sure that the computers at Site B haveInternet access. If this procedure does not solve the problem, talk to a service person at your ISP.

2   If you can ping the external address of each Firebox X Edge, try to ping a local address in the remote network.

From Site A, ping 192.168.111.1. If the VPN tunnel is up, the remote Firebox X Edge sends the ping back. If the ping does not come back, make sure the local configuration is correct. Make sure that the local DHCP address ranges for the two networks connected by the VPN tunnel do not use any of the same IP addresses. The two networks connected by the tunnel must not use the same IP addresses.

How do I obtain a VPN upgrade license key?

You can purchase a license key for an upgrade from a reseller or from the WatchGuard Web site:

http://www.watchguard.com/sales/buyonline.asp

Is the Firebox X Edge compabtible with WatchGuard System Manager?

Yes. The default Firebox X Edge configuration is compatible with WatchGuard System Manager v7.3. To configure the Edge for use with WSM v7.0, v7.1, and v7.2, browse to the VPN Manager Access

page. Select the checkbox **Compatible with pre WFS v.3 VPN Manager.**

CHAPTER 10 Configuring the MUVPN Client

The MUVPN client is a software application that is installed on a remote computer. The client makes a secure connection from the remote computer to your protected network on an unsecured network. The MUVPN client uses Internet Protocol Security (IPSec) to secure the connection.

This example shows how the MUVPN client is used.

- The MUVPN client is installed on a remote computer.
- The user connects to the Internet with the remote computer. The user starts the MUVPN client.
- The MUVPN client creates an encrypted tunnel to the Firebox X Edge.
- The Firebox X Edge connects the remote computer to the trusted network. The employee has secure remote access to the internal network.

The MUVPN client includes ZoneAlarm®, a software firewall. ZoneAlarm gives remote computers more security. The use of ZoneAlarm is optional.

This chapter shows how to install and configure the MUVPN client on a remote computer. This chapter also includes information about the features of the ZoneAlarm personal firewall.

Preparing Remote Computers to Use the MUVPN Client

Install the MUVPN client only on computers that have these minimum requirements.

System requirements

- A computer with a Pentium processor (or equivalent)
- Compatible operating systems and minimum RAM:
  - Microsoft Windows 98: 32 MB
  - Microsoft Windows ME: 64 MB
  - Microsoft Windows NT 4.0 Workstation: 32 MB
  - Microsoft Windows 2000 Professional: 64 MB
  - Microsoft Windows XP: 64 MB
- We recommend that you install the newest Service Packs for each operating system
- 10 MB hard disk space
- Native Microsoft TCP/IP communications protocol
- Microsoft Internet Explorer 5.0 or later
- An Internet service provider account
- A dial-up or broadband (DSL or cable modem) connection

To use Windows file and print sharing on a MUVPN tunnel, the remote computer must contact the WINS and DNS servers. These servers are on the Firebox X Edge trusted network. To contact these servers, the Windows components must be configured on the remote computer.

Windows 98/ME setup

Use this section to install and configure the network components for the Windows 98/ME operating system. You must install these components before the MUVPN client can function correctly on a Windows 98/ME computer.

Configuring network names

From the Windows desktop:

1   Select **Start > Settings > Control Panel**.

2   Double-click the **Network** icon.
     The Network window appears.

3   Make sure the Client for Microsoft Networks is installed.
     Install the Client for Microsoft Networks before you use this procedure
     to configure network names. See "Installing the Client for Microsoft
     Networks" on page 123 for more information.

4   Click the **Identification** tab.

5   Type a name for the remote computer.
     This name must be unique on the remote network.

6   Type the domain name for this connection.

7   Type a description for the remote computer.
     This step is optional.

8   Click **OK** to close the Network window.
     Click Cancel to discard your changes.

9   Restart the computer.

Installing the Client for Microsoft Networks

To install the Client for Microsoft Networks, from the Network window:

1   Click the **Configuration** tab and click **Add**.
     The Select Network Component Type window appears.

2   Select **Client** and click **Add**.
     The Select Network Client window appears.

3   Select **Microsoft** from the list. Select **Client for Microsoft
     Networks** from the list and click **OK**.

4   Select **Client for Microsoft Networks** and click **Properties**.

5   Select the **Log on to Windows NT domain** checkbox.

6   Type the domain name in the **Windows NT Domain** field.
     Examples of typical domain names are "sales", "office", and "warehouse".

7   Select the **Logon and Restore Network Connections** checkbox.

Installing Dial-Up Networking

You must install Dial-Up Networking before the Mobile User VPN
Adapter is installed. If Dial-up Networking is not installed, use this
procedure.

From the Windows desktop:

1   Select **Start > Settings > Control Panel**.

2   Double-click the **Add/Remove Programs** icon.
The Add/Remove Properties window appears.

3   Click the **Windows Setup** tab.
The Windows Setup dialog box appears. Windows looks for installed
components.

4   Select the **Communications** checkbox and then click **OK**.
The **Copying Files** dialog box appears. The operating system copies the
necessary files.

5   The Dial-Up Networking Setup window appears. Click **OK** to
restart the computer.
The computer reboots.

The Dial-up Networking 1.4 version patch must be installed if you
use Windows 98. Get this update from the Microsoft Web site.

Configuring the WINS and DNS settings

The remote computer must be able to contact the WINS and DNS
servers. These servers are on the trusted network of the Firebox X
Edge.

From the Windows desktop:

1   Select **Start > Settings > Control Panel**.

2   Double-click the **Network** icon.
The Network window appears.

3   Select **TCP/IP > Dial–Up Adapter** and then click **Properties**.
The TCP/IP Properties Information window appears.

4   Click **OK**.

5   Click the **DNS Configuration** tab and select the **Enable DNS**
checkbox.

6   Type the IP address of the DNS server in the **DNS Server Search
Order** text field. Click **Add**.
If you have more than one remote DNS server, repeat steps 5 and 6 for
each server.

——————————— **NOTE** ———————————
The DNS server on the private network of the Firebox X Edge must
be the first server in the list.

7   Click the **WINS Configuration** tab and select the **Enable WINS
Resolution** checkbox.

8   Type the IP address of the WINS server in the **WINS Server Search Order** text field and click **Add**.
If you have more than one remote WINS server, repeat steps 7 and 8 for each server.

9   Click **OK** to close the TCP/IP Properties window. Click **OK** to close the Network window.
The **System Settings Change** dialog box appears.

10   Click **Yes** to restart the computer.
The computer restarts.

Windows NT setup

Use this section to install and configure the network components for the Windows NT operating system. These components must be installed before you can use the MUVPN client on a Windows NT computer.

Installing Remote Access Services on Windows NT

You must install Remote Access Services (RAS) before you install the Mobile User VPN Adapter. To install RAS, use this procedure.

1   Follow the Windows desktop, select **Start > Settings > Control Panel**.

2   Double-click the **Network** icon.
The Network window appears.

3   Click the **Services** tab and click **Add**.

4   Select **Remote Access Services** and click **OK**.

5   Type the path to the Windows NT installation files, or put your system installation CD in the computer and click **OK**.
The **Remote Access Setup** window appears.

6   Click Y**es t**o add a RAS device, for example, a modem, and then click Add.

7   Complete the Install New Modem wizard.

───────────────── **NOTE** ─────────────────
If there is no modem installed, select the **Don't detect my modem; I will select it from a list** checkbox. Select the standard 28800 modem. If a modem is not available, you can select **a serial cable between two computers**.
──

8   Select the modem from the Add RAS Device window.

9   Click **OK**, click **Continue** and click **Close**.

10 Restart the computer.

Configuring the WINS and DNS settings

The remote computer must be able to contact the WINS servers and the DNS servers. These servers are located on the trusted network that is protected by the Firebox X Edge.

From the Windows desktop:

1 Select **Start > Settings > Control Panel**.

2 Double-click the **Network** icon.
   The Network window appears.

3 Click the **Protocols** tab and select the **TCP/IP** protocol.

4 Click **Properties**.
   The Microsoft TCP/IP Properties window appears.

5 Click the **DNS** tab and click **Add**.

6 Type the IP address of your DNS server.
   To add more DNS servers, repeat steps 5 and 6 for each server.

─── **NOTE** ───

The DNS server on the private network of the Firebox X Edge must be the first server in the list.

7 Click the **WINS Address** tab, type the IP address of your WINS server in the applicable field, and then click **OK**.
   To add more WINS servers, repeat this step.

8 Click **Close** to close the Network window.
   The Network Settings Change dialog box appears.

9 Click **Yes** to restart the computer.
   The computer restarts.

Windows 2000 setup

Use this section to install and configure the network components for the Windows 2000 operating system. These components must be installed before you can use the MUVPN client on a Windows 2000 computer.

From the Windows desktop:

1 Select **Start > Settings > Network and Dial-up Connections**.

2 Select the dial-up connection you use to get Internet access.
   The connection window appears.

3 Click **Properties** and click the **Networking** tab.

4   Make sure the following components are installed and enabled:
- Internet Protocol (TCP/IP)
- File and Printer Sharing for Microsoft Networks
- Client for Microsoft Networks

Installing the Internet Protocol (TCP/IP) network component

From the connection window **Networking** tab:

1   Click **Install.**
The **Select Network Component Type** window appears.
2   Double-click the **Protocol** network component.
The **Select Network Protocol** window appears.
3   Select the **Internet Protocol (TCP/IP)** network protocol. Click **OK.**

Installing the File and Printer Sharing for Microsoft Networks

From the connection window Networking tab:

1   Click **Install.**
The **Select Network Component Type** window appears.
2   Double-click the **Services** network component.
The **Select Network Service** window appears.
3   Select the **File and Printer Sharing for Microsoft Networks** network service and click **OK.**

Installing the Client for Microsoft Networks

From the connection window Networking tab:

1   Click **Install.**
The **Select Network Component Type** window appears.
2   Double-click the **Client** network component.
The **Select Network Protocol** window appears.
3   Select the **Client for Microsoft Networks** network client and click **OK.**

Configuring the WINS and DNS settings

The remote computer must be able to contact the WINS and DNS servers. These servers are on the trusted network of the Firebox X Edge.

From the connection window Networking tab:

1 Select the **Internet Protocol (TCP/IP)** component and click
   Properties.
   The **Internet Protocol (TCP/IP) Properties** window appears.

2 Click **Advanced.**
   The **Advanced TCP/IP Settings** window appears.

3 Click the **DNS** tab and from the section labeled **DNS server
   addresses, in order of use**, click **Add.**
   The TCP/IP DNS Server window appears.

4 Type the IP address of the DNS server and click **Add.**
   To add more DNS servers, repeat steps 3 and 4.

   ──────────────── **NOTE** ────────────────
   The DNS server on the private network of the Firebox X Edge must
   be the first server in the list.
   ───

5 Select the **Append these DNS suffixes (in order)** checkbox and
   click **Add.**
   The **TCP/IP Domain Suffix** window appears.

6 Type the domain suffix in the applicable field.
   To add additional DNS suffixes, go back to step 5.

7 Click the **WINS** tab and then from the section **WINS addresses,
   in order of use**, click **Add.**
   The TCP/IP WINS Server window appears.

8 Type the IP address of the WINS server in the applicable field.
   Click **Add.**
   To add more WINS servers, repeat steps 7 and 8.

9 Click **OK** to close the Advanced TCP/IP Settings window. Click
   OK to close the Internet Protocol (TCP/IP) Properties window.

10 Click **OK.**

11 Click **Cancel** to close the connection window.

Windows XP setup

Use this section to install and configure the network components
for the Windows XP operating system. You must install these com-
ponents if you use the MUVPN Client on a Windows XP computer.

From the Windows desktop:

1 Select **Start > Control Panel**
   The Control Panel window appears.

2   Double-click the **Network Connections** icon.

3   Double-click the connection you use to get Internet access.
     The connection window appears.

4   Click **Properties** and then click the **Networking** tab.

5   Make sure the following components are installed and enabled:
     - Internet Protocol (TCP/IP)
     - File and Printer Sharing for Microsoft Networks
     - Client for Microsoft Networks

Installing the Internet Protocol (TCP/IP) Network Component

From the connection window Networking tab:

1   Click **Install**.
     The Select Network Component Type window appears.

2   Double-click the **Protocol** network component.
     The Select Network Protocol window appears.

3   Select the **Internet Protocol (TCP/IP)** network protocol. Click
     OK.

Installing the File and Printer Sharing for Microsoft Networks

From the connection window, Networking tab:

1   Click **Install**.
     The Select Network Component Type window appears.

2   Double-click the **Services** network component.
     The Select Network Service window appears.

3   Select the **File and Printer Sharing for Microsoft Networks**
     network service. Click **OK**.

Installing the Client for Microsoft Networks

From the connection window Networking tab:

1   Click **Install**.
     The Select Network Component Type window appears.

2   Double-click the **Client** network component.
     The Select Network Protocol window appears.

3   Select the **Client for Microsoft Networks** network client. Click
     OK.

Configuring the WINS and DNS settings

The remote computer must be able to contact the WINS and DNS servers. These servers are on the trusted network of the Firebox X Edge.

From the connection window, Networking tab:

1   Select the **Internet Protocol (TCP/IP)** component.

2   Click **Properties**.
    The Internet Protocol (TCP/IP) Properties window appears.

3   Click **Advanced**.
    The Advanced TCP/IP Settings window appears.

4   Click the **DNS** tab and then, from the section labeled **DNS server addresses, in order of use**, click **Add**.
    The TCP/IP DNS Server window appears.

5   Type the IP address of the DNS server in the applicable field. Click **Add**.
    To addmore DNS servers, repeat steps 4 and 5.

─────────────── **NOTE** ───────────────
The DNS server on the private network of the Firebox X Edge must be the first server in the list.

6   Select the **Append these DNS suffixes (in order)** checkbox. Click **Add**.
    The TCP/IP Domain Suffix window appears.

7   Enter the domain suffix in the applicable field.
    To add more DNS suffixes, repeat step 6.

8   Click the **WINS** tab and in the section labeled **WINS addresses, in order of use**, click **Add**.
    The TCP/IP WINS Server window appears.

9   Type the IP address of the WINS server in the applicable field. Click **Add**.
    To add more WINS servers, repeat steps 8 and 9.

10 Click **OK** to close the Advanced TCP/IP Settings window. Click **OK** to close the Internet Protocol (TCP/IP) Properties window, and then click **OK**.

11 Click **Cancel** to close the connection window.

Installing and Configuring the MUVPN Client

Get the MUVPN installation files from the WatchGuard Web site:
http://www.watchguard.com/support

─── **NOTE** ───

To install and configure the MUVPN client, you must have local administrator rights on the remote computer.

Installing the MUVPN client

To install the MUVPN client:

1   Copy the MUVPN installation file to the remote computer.

2   Double-click the MUVPN installation file to start the InstallShield wizard.

3   Click **Next**.
    If the InstallShield stops because of a read-only files error, click Y**es** to continue the installation.

4   A welcome message appears. Click **Next**.
    The Software License Agreement appears.

5   Click **Yes** to accept the License Agreement.
    The Setup Type window appears.

6   Select the type of installation. WatchGuard recommends that you use the Typical installation. Click **Next**.

7   On a Windows 2000 computer, the InstallShield looks for the Windows 2000 L2TP component. If the component is installed, the InstallShield does not install it again. Click **OK** to continue.
    The Select Components window appears.

8   Do not change the default selections. Click **Next**.
    The Start Copying Files window appears.

9   Click **Next** to install the files.
    When the dni_vapmp file is installed, a command prompt window appears. This is normal. After the file is installed, the command window closes and the installation is continued.

10 After the installation is complete, click **Finish**.

11 The InstallShield wizard looks for a user profile. Click **Next** to skip this step. You do not need to have an installed user profile.
    An information dialog box appears.

12 Click **OK** to continue the installation.

13 The MUVPN client is installed. Make sure the option **Yes, I want to restart my computer now** is selected. Click **Finish**.
The computer restarts.

──────────────── **NOTE** ────────────────
The ZoneAlarm personal firewall may prevent you from conencting to the network after the computer restarts. If this occurs, log on to the computer locally the first time after installation. For more information, see "The ZoneAlarm Personal Firewall" on page 140.

Importing the .wgx file

The Firebox X Edge has encrypted MUVPN client configuration (.wgx) files available for download.

1 To connect to the System Status page, type the IP address of the trusted network in the browser.
The default IP address is: https://192.168.111.1

2 From the navigation bar, select **Firebox Users** and scroll to the bottom of the page.

3 Under **MUVPN Client Configuration Files,** select the .wgx file you want to download and follow the instructions on the screen.

Secure MUVPN Client Configuration Files

External MUVPN access count 0 (maximum 15)

The following secure (encrypted) MUVPN client configuration (.wgx) files are available for download. Once downloaded, these files can be used to configure your MUVPN client software in a manner that is consistent with the currently defined MUVPN settings on the X15.

Account Name	MUVPN Client Configuration Files
admin	admin.wgx
muvpn	muvpn.wgx
user	user.wgx
cfgview	cfgview.wgx

Uninstalling the MUVPN client

Use this procedure to uninstall the MUVPN client. WatchGuard recommends that you use the Windows Add/Remove Programs tool.

Disconnect all existing tunnels and dial-up connections. Reboot the remote computer. From the Windows desktop:

1   Select **Start > Settings > Control Panel.**
    The Control Panel window appears.

2   Double-click the **Add/Remove Programs** icon.
    The Add/Remove Programs window appears.

3   Select **Mobile User VPN** and click **Change/Remove**.
    The InstallShield wizard appears.

4   Select **Remove**. Click **Next**.
    The Confirm File Deletion dialog box appears.

5   Click **OK** to remove all of the components.
    When the dni_vapmp file is removed, a command prompt window appears. This is normal. After the file is removed, the command prompt window closes and the procedure continues.
    The Uninstall Security Policy dialog box appears.

6   Click **Yes** to delete the Security Policy Personal Certificates and the Private/Public Keys.
    The InstallShield Wizard window appears.

7   Select the **Yes, I want to restart my computer now**. Click the **Finish** option.
    The computer reboots.

--- **NOTE** ---

The ZoneAlarm personal firewall settings are stored in the following directories by default.

Windows 98: c:\windows\internet logs\
Windows NT and 2000: c:\winnt\internet logs\
Windows XP: c:\windows\internet logs

To remove these settings, delete the contents of the appropriate directory.

8   When the computer has restarted, select **Start > Programs**.

9   Right-click **Mobile User VPN** and select **Delete** to remove this selection from your **Start** menu.

Enabling MUVPN for Edge Users

After you have configured the MUVPN client, you can configure MUVPN client and user settings on the Firebox X Edge.

Configuring MUVPN client settings

The MUVPN client settings apply to all of the Edge's MUVPN connections. For information on these settings, see "Configuring MUVPN client settings" on page 151.

Enabling MUVPN access for an Edge user account

1   Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
    The default trusted IP address is https://192.168.111.1.

2   Add a new user or edit an existing user, as described in "Adding or Editing a User Account" on page 152.

3   Click the **MUVPN** tab.

4   Select the **Enable MUVPN for this account** checkbox.

5   Type a shared key in the applicable field.

6   Type the virtual IP address in the applicable field.
    The virual IP address must be an address on the Firebox X Edge trusted network that is not used. This address is used by the remote computer to connect to the Firebox X Edge.

7   From the **Authentication Algorithm** drop-down list, select the type of authentication.
    The options are MD5-HMAC and SHA1-HMAC.

8   From the **Encryption Algorithm** drop-down list, select the type of encryption.
    The options are DES-CBC and 3DES-CBC.

9   Set MUVPN key expiration in kilobytes or hours. The default values are 8192 KB and 24 hours, respectively.

10 Select **Mobile User** from the **VPN Client Type** drop-down list.

11 Select the **All traffic uses tunnel (0.0.0.0/0 IP Subnet)** checkbox if the remote client will send all its traffic (including normal Web traffic) over the VPN to the Firebox X Edge. This can also let the MUVPN client communicate with other networks that the Firebox X Edge connects. If this checkbox is selected, the MUVPN client software must be configured with the subnet and mask fields set to 0.0.0.0.

12 Click **Submit**.

Configuring the Firebox for MUVPN Clients Using Pocket PC

To create a MUVPN tunnel between the Firebox X Edge and your Pocket PC, you must configure the MUVPN Clients feature on the Firebox. Follow the previous procedure, except select **Pocket PC** from the **VPN Client Type** drop-down list.

For additional information about configuring your Pocket PC to serve as an MUVPN client, go to the WatchGuard Web site:

https://www.watchguard.com/support/sohoresources/soinstallhelp.asp

Connecting and Disconnecting the MUVPN Client

The MUVPN client software makes a secure connection from a remote computer to your protected network on the Internet. To start this connection, you must connect to the Internet and use the MUVPN client to connect to the protected network.

Connecting the MUVPN client

1   Start your connection to the Internet through a Dial-Up Networking connection, a LAN connection, or a WAN connection.

From the Windows desktop system tray:

2   If the MUVPN client is not active, right-click the icon and select
     Activate Security Policy.
     For information about the MUVPN icon, see "The MUVPN client icon" on
     page 136.

From the Windows desktop:

3   Select **Start > Programs > Mobile User VPN > Connect**.
     The WatchGuard Mobile User Connect window appears.

4   Click **Yes**.

The MUVPN client icon

The MUVPN icon appears in the Windows desktop system tray. The
icon image provides information about the status of the connection.

Deactivated

The MUVPN Security Policy is not active. This icon can appear if
the Windows operating system did not start a required MUVPN
service. If this occurs, the remote computer must be restarted. If
the problem continues, reinstall the MUVPN client.

Activated

The MUVPN client can make a secure MUVPN tunnel
connection.

Activated and Transmitting Unsecured Data

The MUVPN client can make a secure MUVPN tunnel
connection. The red bar on the right of the icon tells you that
the client is sending data that is not secure.

Activated and Connected

The MUVPN client is connected with one or more secure MUVPN
tunnels, but it is not sending data.

Activated, Connected and Transmitting Unsecured Data

The MUVPN client started one or more secure MUVPN tunnel connections. The red bar on the right of the icon tells you that the client is sending data that is not secure.

Activated, Connected and Transmitting Secured Data

The MUVPN client started one or more secure MUVPN tunnels. The green bar on the right of the icon tells you that the client is only sending data that is secure.

Activated, Connected and Transmitting both Secured and Unsecured Data

The MUVPN client started one or more secure MUVPN tunnels. The green and red bars on the right of the icon tell you that the client is sending data that is secure and data that is not secure.

Allowing the MUVPN client through a personal firewall

To create the MUVPN tunnel, you must allow these programs through the personal firewall:

• MuvpnConnect.exe

• IrelKE.exe

The personal firewall detects when these programs attempt to access the Internet. A New Program alert window appears to request access for the MuvpnConnect.exe program.

From the New Program alert window:

1   Select the **Remember this answer the next time I use this program** checkbox, then click **Yes**.
    This option lets the ZoneAlarm personal firewall allow Internet access for this program each time you start a MUVPN connection.
    The New Program alert window appears to request access for the IrelKE.exe program.

2   Set the **Remember this answer the next time I use this program** check box and then click **Yes**.
This option lets the ZoneAlarm personal firewall allow Internet access for this program each time you start a MUVPN connection.

Disconnecting the MUVPN client

From the Windows desktop system tray:

1   Right-click the MUVPN client icon and select **Deactivate Security Policy**.
The MUVPN client icon with a red bar is displayed.
If the ZoneAlarm personal firewall is active, deactivate it now.

From the Windows desktop system tray:

1   Right-click the ZoneAlarm icon shown at right. ZA

2   Select **Shutdown ZoneAlarm**.
The ZoneAlarm window appears.

3   Click **Yes**.

Monitoring the MUVPN Client Connection

The Log Viewer and the Connection Monitor are installed with the MUVPN client. These tools let you monitor the MUVPN connection and troubleshoot problems.

Using Log Viewer

Use Log Viewer to display the communications log. This log shows the events that occurr when the MUVPN tunnel is started.

From the Windows desktop system tray:

1   Right-click the **Mobile User VPN** client icon.

2   Select **Log Viewer**.
The Log Viewer window appears.
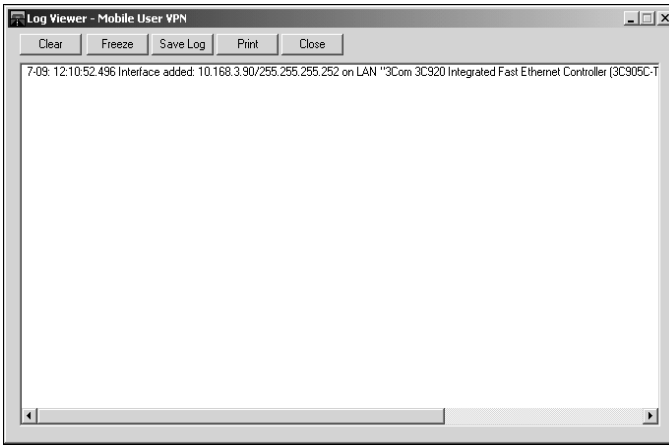
Using Connection Monitor

The Connection Monitor shows statistical and diagnostic information for connections in the security policy. This window shows the security policy settings and the security association (SA) information. The monitor records the information that appears in this window during the phase 1 IKE negotiations and the phase 2 IPSec negotiations.

From the Windows desktop system tray:

1   Right-click the **Mobile User VPN** client icon.

2   Select **Connection Monitor.**
     The Connection Monitor window appears.
An icon appears to the left of the connection name:

• SA tells you that the connection only has a phase 1 SA. A phase 1 SA is assigned in the following situations:
   - for a connection to a secure gateway tunnel
   - when a phase 2 SA connection has not yet been made
   - when a phase 2 SA connection cannot be made

• A key tells you that the connection has a phase 2 SA. This connection may also have a phase 1 SA.

• An animated black line underneath a key tells you that the client is processing secure IP traffic.

- A single SA icon with several key icons above it indicates a single phase 1 SA to a gateway that protects multiple phase 2 SAs.

The ZoneAlarm Personal Firewall

ZoneAlarm Personal firewall protects your computer and network by following a simple rule: Block all incoming and outgoing traffic unless you explicitly allow that traffic for trusted programs.

When you use ZoneAlarm you often see New Program alert windows. This alert appears when an application tries to get Internet or local network access. This alert stops data from your computer without your authorization.

The ZoneAlarm personal firewall includes a tutorial after the MUVPN client is installed. Read the tutorial to learn how to use this application.

For more information about the features and configuration of ZoneAlarm, use the ZoneAlarm help system. To access the help system, select **Start > Programs > Zone Labs > ZoneAlarm Help**.

Allowing traffic through ZoneAlarm

When an application tries to get access through the ZoneAlarm personal firewall, a New Program alert appears. This alert tells the user the name of the application. This can cause confusion for users.

To let a program get access to the Internet each time the application is started, select the **Remember the answer each time I use this program** check box.

Here is a list of some programs that need to pass through the ZoneAlarm personal firewall when you use their associated applications.

Programs That Must Be Allowed	
MUVPN client	IreIKE.exe MuvpnConnect.exe
MUVPN Connection Monitor	CmonApp.exe
MUVPN Log Viewer	ViewLog.exe
Programs That Can be Allowed	
MS Outlook	OUTLOOK.exe

MS Internet Explorer	IEXPLORE.exe
Netscape 6.1	netscp6.exe
Opera Web browser	Opera.exe
Standard Windows network applications	lsass.exe services.exe svchost.exe winlogon.exe

Shutting down ZoneAlarm

From the Windows desktop system tray:

1 Right-click the ZoneAlarm icon shown at right. **ZA**

2 Select **Shutdown ZoneAlarm**.
The ZoneAlarm window appears.

3 Click **Yes**.

Uninstalling ZoneAlarm

From the Windows desktop:

1 Select **Start** > **Programs** > **Zone Labs** > **Uninstall ZoneAlarm**.
The Confirm Uninstall dialog box appears.

2 Click **Yes**.
The ZoneLabs TrueVector service dialog box appears.

3 Click **Yes**.
The Select Uninstall Method window appears.

4 Make sure **Automatic** is selected and then click **Next**.

5 Click **Finish**.

――――――――――― **NOTE** ―――――――――――
The Remove Shared Component window can appear. During the
initial installation of ZoneAlarm, some files were installed that
could be shared by other programs on the system. Click **Yes to All**
to completely remove all of these files.

6 The Install window appears and prompts you to restart the
computer. Click **OK** to restart.

Troubleshooting Tips

Get additional information about the MUVPN client from the WatchGuard Web site:

www.watchguard.com/support

The answers to several frequently asked questions about the MUVPN client are answered below.

My computer hangs immediately after installing the MUVPN client…

This problem can be caused by one of the following two problems:

- The ZoneAlarm personal firewall application is stopping normal traffic on the local network.

- The MUVPN client is active and is unsuccessfully attempting to create VPN tunnels.

When the MUVPN client is not in use, ZoneAlarm and the MUVPN client should be deactivated.

From the Windows desktop system tray:

1   Reboot your computer.

1   Right-click the MUVPN client icon and select **Deactivate Security Policy**.
    The MUVPN client icon with a red bar appears to indicate that the Security Policy has been deactivated.

1   Right-click the ZoneAlarm icon shown at right. ZA

2   Select **Shutdown ZoneAlarm**.
    The ZoneAlarm dialog box appears.

3   Click **Yes**.

I have to enter my network login information even when I'm not connected to the network…

When you start your computer, you must type your Windows network user name, password, and domain. It is very important that you type this information correctly. Windows keeps this information for use by network adapters and network applications. When you connect through the MUVPN client, your computer uses this information to connect to the company network.

I am not prompted for my user name and password when I turn my computer on...

The ZoneAlarm personal firewall application can cause this problem. This program is very good at what it does. ZoneAlarm keeps your computer secure from unauthorized incoming and outgoing traffic. Unfortunately, it can prevent your computer from broadcasting its network information. This prevents your computer from sending the login information. Make sure you deactivate ZoneAlarm each time you disconnect the MUVPN connection.

Is the MUVPN tunnel working?

The MUVPN client icon appears in the Windows desktop system tray when the application is launched. The MUVPN client displays a key in the icon when the client is connected.

To test the connection, ping a computer on your company network.

- Select **Start > Run** and then type `ping` and the IP address of a computer on your company network.

My mapped drives have a red X through them...

Windows 98/ME, NT, and 2000 verify and map network drives automatically when the computer starts. Because you cannot establish a remote session with the company network before the computer starts, this process fails. This causes a red X to appear on the drive icons. To correct this problem, start a MUVPN tunnel and open the network drive. The red X for that drive should disappear.

How do I map a network drive?

Due to a Windows operating system limitation, mapped network drives must be remapped when you work remotely. To remap a network drive from the Windows desktop:

1 Right-click **Network Neighborhood**.

2 Select **Map Network Drive**.
   The Map Network Drive window appears.

3 Use the drop-down list to select a drive letter.
   Select a drive from the drop-down list or type a network drive path.

4 Click **OK**.

The mapped drive appears in the My Computer window. Even if you select the **Reconnect at Logon** checkbox, the mapped drive will only appear the next time you start your computer if the computer is directly connected to the network.

I am sometimes prompted for a password when I am browsing the company network...

Due to a Windows networking limitation, remote user virtual private networking products can allow access only to a single network domain. If your company has multiple networks connected together, you will only be able to browse your own domain. If you try to connect to other domains, a password prompt will appear. Unfortunately, even providing the correct information will not allow you to access these additional networks.

It takes a *very* long time to shut down the computer after using the MUVPN client...

If you access a mapped network drive during an MUVPN session, the Windows operating system will wait for a signal from the network before the shutdown is complete.

I lost the connection to my ISP, and now I can't use the company network...

If your Internet connection is interrupted, the connection to the MUVPN tunnel may be lost. Follow the procedure to close the tunnel. Reconnect to the Internet. Restart the MUVPN client.

Managing the Firebox® X Edge

The Firebox® X Edge includes tools to help you manage your network and your users. You can:

- Examine current users and properties
- Configure user profiles and customize user accounts
- Upgrade the Edge and activate new features
- Examine the current configuration file in a text format

Viewing Current Sessions and Users

A *session* is a connection between a computer on the trusted or optional network and a computer on the external network. For example when a user on your trusted network opens a browser to connect to a Web site on the Internet, a session starts on the Firebox® X Edge. On the Firebox Users page, you can see information in the **Active Sessions** section. You can also see information on the users that you configured for this Edge.

1 To connect to the System Status page, type the IP address of the trusted network in the browser.
   The default IP address is: https://192.168.111.1

2   From the navigation bar, select **Firebox Users**.
The Firebox Users page appears.

Firebox Users

Firebox User Settings

Firebox User accounts are disabled   Configure

    Restrict External Network access: Disabled
    Restrict VPN tunnel access: Disabled
    Enforce session idle time-out: Disabled
    Enforce maximum access time: Disabled
    Reset idle on Firebox X Edge access: Disabled
Periodic automatic global session time-out is disabled

Active Sessions

Active session count is 1 (maximum is 15).
The following sessions are currently active on this Firebox.

User	Host	Close
admin	192.168.111.2	✕

Close All

Local User Accounts

The following local user accounts have
been defined for this Firebox.   Add...

Name	Admin Level	WebBlocker	MUVPN	Edit	Delete
admin	Full	None	Disabled	▣	⊘
new	None	restricted	Disabled	▣	✕
sms	None	None	Disabled	▣	✕

Secure MUVPN Client Configuration Files

The count of configured MUVPN clients is 0 (15 external).

Firebox User Settings

Below **Firebox User Settings**, you can see the current values for all global user and session settings. Click the **Configure** button to open the Settings page. For more information, see "Changing authentication options for all users" on page 149 and "Configuring MUVPN client settings" on page 151.

Active Sessions

An active session is a connection from the trusted or optional network through the Firebox to the external network. The Firebox uses one seat license for each active session. Below **Active Sessions**, the page shows information for all current sessions:

• The name of the user who started the session

- The total length of time of the session
- The time between the last packet and the session expiration. This is known as the idle time. If you set the idle time to 0 hours and 0 minutes, the Firebox does not disconnect the session.

Closing a session

To disconnect an active session, click the **X** for the session. A dialog box appears. Click **Yes** to disconnect the session. To disconnect all active sessions, click **Close All**.

- The user can log out manually by clicking the **Logout** button on [page]. If the user clicks this button, the Login Status box closes, and a warning dialog bog appears. The logout process is not complete until the user closes all open browsers.

When a session closes, the seat license is available again for another user. For more information on seat licenses, see "About Seat Licenses" on page 156.

Local User Accounts

Below **Local User Accounts**, you can see information on the users you configured to use this Edge:

- Name -- The administrator account appears first in the list. Other users appear in alphanumeric sequence.
- Admin Level -- You can set the user permissions to Full, None, or Read-only. For more information, see "Adding or Editing a User Account," on page 152.
- Options -- You can configure a user to use WebBlocker or MUVPN. For more information, see "Setting a WebBlocker profile for a user," on page 154 and "Enabling MUVPN for a user," on page 154.

Editing a user account

To edit a user account, click its **Edit** icon. For descriptions of the fields you can configure, see "Adding or Editing a User Account," on page 152.

Local User Accounts							
The following local user accounts have been defined for this Firebox.							Add...
Name	Internet Access	Admin Level	WebBlocker	MUVPN	VPN	Edit	Delete
admin	Allow	Full	None	Disabled	Allow	🖳	⊘
testuser	Allow	None	None	Disabled	Allow	🖳	✕
scarlson	Allow	Full	None	Disabled	Allow	🖳	✕

Deleting a user account

To remove a user account, click the **X** for the account. A dialog box appears. Click **Yes** to remove the account.

Local User Accounts							
The following local user accounts have been defined for this Firebox.							Add...
Name	Internet Access	Admin Level	WebBlocker	MUVPN	VPN	Edit	Delete
admin	Allow	Full	None	Disabled	Allow	🖳	⊘
testuser	Allow	None	None	Disabled	Allow	🖳	✕
scarlson	Allow	Full	None	Disabled	Allow	🖳	✕

About User Authentication

The Firebox® X Edge uses advanced authentication options to increase network security. There are options to prevent connections to some resources and to help decrease the number of seat licenses necessary. This section gives information on how a user can authenticate to the Edge, how your users and administrators can close an active session, and which options are available to customize authentication.

There are three levels of Administrative Access available for the Edge:

• **None** -- Use to connect to resources on the external network. A user with this access level can not see or change the Edge configuration pages.

- **Read-Only** -- Use to see Edge configuration properties and status. A user with this access level can not change the configuration file.

- **Full** -- Use to see and to change Edge configuration properties. You can also activate options, disconnect active sessions, restart the Edge, and add or edit user accounts. A user with this access level can change the passphrase for all user accounts.

Authenticating to the Firebox

When you authenticate to the Edge, it automatically identifies your Administrative Access Level. The authentication procedure is the same for all users.

1 Open a Web browser.
   You can use Netscape Navigator or Microsoft Internet Explorer. The Edge may be compatible with other Web browsers, but we do not support them.
2 Type the Firebox X Edge trusted IP address in the address bar. The factory default trusted IP address address is:
   https://192.168.111.1.

3 A security dialog box appears. You must accept the warning before you can continue.

When you authenticate to the Edge, one of two screens appears. A user with Read-Only or Full Administrative Access sees the Firebox X Edge System Status page. A user with Administrative Access set to None sees a dialog box with an authentication status message.

When you authenticate to the Edge, your user name appears in the **Active Sessions** section of the Firebox Users page.

Changing authentication options for all users

There are some authentication settings which apply to all users. To change authentication options:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox.
   The default IP address is: https://192.168.111.1
2 From the navigation bar, select **Firebox > Settings**.
   The Settings page appears.

3 Use the definitions below to help you change your settings. Click **Submit**.

```
Firebox Users
Settings

Firebox User Access Restriction Enforcement and Options
☐  Require user authentication (enable local user accounts).
   ☑ Enforce External Network access restrictions.
   ☑ Enforce VPN tunnel access restrictions.
   ☑ Enforce idle time-out.
   ☑ Enforce maximum access time.
   ☑ Reset idle timer on Firebox X Edge embedded Web site access.
☐  Enable automatic session termination every |hour    ▼|

Firebox User Common MUVPN Client Settings

The following settings apply to all MUVPN clients.

☐  Make the MUVPN client security policy read-only.
          Virtual Adapter |Preferred ▼|
      DNS Server Address |            |  [optional]
     WINS Server Address |            |  [optional]

[ Submit ]  [ Reset ]
```

- **Require User Authentication –** You must select this check box to use the authentication options.

- **External Network Access Restrictions** – Enable this check box if it is necessary for your users to authenticate before they connect to computers on the external network. The external network is frequently the Internet.

- **VPN Tunnel Access Restrictions** – Enable this check box if it is necessary for your users to authenticate before they can connect to computers on different network through a branch office VPN.

- **Idle Time-Out** – When the user does not send traffic to the external network for the length of the idle time-out, the Edge closes the session.

- **Maximum Access Time** – You can configure the Edge to close a session after a specified interval. Customers frequently use this option to prevent their users from browsing the Internet for extended periods of time. When a user authenticates to the

Edge, the clock starts on the session. After the specified interval, the user must authenticate again or the Edge closes the session.

- **Reset Idle Timer on Embedded Web Site Access** – The Edge will not disconnect a session when an idle time-out occurs if the **Login Status** dialog box is on the desktop. Disable this check box to override the Login Status dialog box.
- **Automatic Session Termination** – This is a global property which applies to all sessions and which overrides all other authentication options. It lets you clear the list of seat licenses in use and make them available again. Enable this check box to disconnect all sessions at the specified time in the drop-down list.

Configuring MUVPN client settings

The MUVPN client settings apply to all MUVPN connections to the Edge. To configure MUVPN client settings:

1 Use your browser to connect to the System Status page. From the navigation bar, select **Firebox Users > Settings**.
The Settings page appears.

2 If necessary, use the scroll bar to scroll to the **Firebox User Common MUVPN Client Settings** section.

3 You can lock the MUVPN client security policy (.wgx file) to prevent a change to it. Select the **Make the MUVPN client security policy read–only** check box.

4 The remote MUVPN computers can use a virtual adapter to get network settings, an IP address, and WINS and DNS. You can set the virtual adapter rule for your mobile users to:

Disabled
The mobile user does not use a virtual adapter to connect with the MUVPN client.

Preferred
If the virtual adapter is in use or it is not available, the mobile user does not use a virtual adapter to connect with the MUVPN client. This is the default value.

Required
The mobile user must use a virtual adapter to connect with the MUVPN client.

5   You can also enter a WINS Server Address and DNS Server
    Address. Type the server IP addresses in the related field.

Adding or Editing a User Account

Firebox X Edge users When you create a user for the Firebox X Edge,
you select the Administrative Access Level for that user. You can also
configure a WebBlocker account and MUVPN restrictions.

1   Type the IP address of the trusted network in your browser
    window to connect to the System Status page of the Firebox.
    The default IP address is: https://192.168.111.1

2   From the navigation bar, select **Firebox Users**.
    The Firebox Users page appears.

3   Under **Local User Accounts**, click **Add**.
    The New User page appears. It shows the Settings tab.

4   In the **Account Name** field, enter a name for the account. The
    user enters this name when authenticating.
    The account name is case-sensitive.

5   In the **Full Name** field, enter the first and last name of the user.
    This is for your information only. A user does not use this name during
    authenticating.

6   In the **Description** field, enter a description for the user.
    This is for your information only.

7   In the **Password** field, enter a password with a maxium of eight
    characters.
    Mix eight letters, numbers, and symbols. Do not use a word you could
    find in a dictionary. For increased security use a minimum of one special
    symbol, a number, and a mixture of uppercase and lowercase letters.

8   Enter the password again in the **Confirm Password** field.

9   In the **Administrative Access** drop-down list, set the level to
    which your user can see and change the Edge configuration
    properties: None, Read-Only, or Full.
    For more information, see "Creating a read only administrative
    account," on page 153.

10 In the **Session maximum time-out** field, set the maximum
    amount of time the user's computer can pass traffic to the
    external network or across a Branch Office VPN. A setting of
    zero minutes means this user has no time limit on how long his
    or her session can last.
    You can also apply a global "Maximum session time-out" to all users. The
    global setting overrides the individual Firebox User setting. For more
    information, see "Changing authentication options for all users" on
    page 149.

11 In the **Session idle time-out** field, set the amount of time the
    user's computer can remain authenticated when it is idle (not
    passing any traffic to the external network or across the Branch
    Office VPN or to the Firebox X Edge itself). A setting of zero
    minutes means there is no idle time-out.

12 If you want this user to have Internet access, select the **Allow
    access to the External Network** checkbox.

13 If you want this user to have access to computers on the other
    side of a Branch Office VPN tunnel, select the **Allow access to
    VPN** checkbox.

14 Click **Submit**.

Creating a read only administrative account

You can create a local user account with limited access to view Fire-
box configuration pages. When you log in as a read-only adminis-
trator, you cannot:

•   Click the **Reboot** button on the System Status page.

- Change the configuration mode on the External page.
- Click the **Reset Event Log** and **Sync Time with Browser Now** buttons on the Logging page.
- Click the **Synchronize Now** button on the System Time page.
- Click the **Regenerate IPSec Keys** button on the VPN page.
- Change the configuration mode on the Managed VPN page.
- Click the **Launch Wizard** button from the Wizard page.

To create a read-only user account, edit the user account. Use the **Administrative Access** drop-down list to select **Read Only**.

Setting a WebBlocker profile for a user

A WebBlocker profile is a unique set of restrictions you can apply to users on your network. To set a WebBlocker profile for a new user, click the WebBlocker tab and select a profile from the drop-down list. For more information on WebBlocker profiles, see "Creating WebBlocker Profiles" on page 99.

Enabling MUVPN for a user

To enable MUVPN for a new user, see "Enabling MUVPN for Edge Users" on page 133.

The Administrator account

The Firebox X Edge has a built-in administrator account that cannot be deleted. You can, however, change some of the administrator account's settings. On the Firebox Users page, click the icon in the **Edit** column of the administrator account.

For descriptions of the fields, see the previous section, "Adding a New User."

Make sure you record the administrator name and password in a safe location. These are required to access the configuration pages. If the system administrator name and password are unknown or you have forgotten them, you must reset the Firebox to the factory default settings. For more information, see "Resetting the Firebox to the factory default settings" on page 42.

We recommend that you change the administrator password every month. Select a combination of eight letters, numbers, and symbols. Do not use an English or foreign word. Use at least one special sym-

bol, a number, and a mixture of upper case and lower case letters for increased security.

Terminating a session

A Firebox uses a session when it makes a connection between a computer on the trusted interface and a computer on the external interface. The Firebox releases the session when:

- the session reaches the idle timeout limit;
- the session reaches the maximum time limit;
- the Firebox administrator uses the Firebox Users page to end the session
- the user ends the session by closing all browser windows; or
- the Firebox restarts.

To end a session manually:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox.
The default IP address is: https://192.168.111.1

2 From the navigation bar, select **Firebox Users**.
The Firebox Users page appears.

3 Find the session in Active Sessions list. Click the close button. To end all sessions, click the **Close All** button.

Changing a user account name or password

You can change either an account name or account password. You cannot change then both. If you change the account name, you must provide the account password.

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox.
The default IP address is: https://192.168.111.1

2 From the navigation bar, select **Firebox Users**.
The Firebox Users page appears.

3 Under **Local User Accounts**, click **Edit** for the account whose password you want to change.
The Edit User page appears with the Settings tab visible.

4 Click **Change Identification**.

5 Type the old password and a new password. Confirm the new password.

6   Click **Submit**.

About Seat Licenses

The Firebox X Edge is enabled with a set number, or "pool," of seat licenses. The number of seat licenses limits how many users can get out to the Internet at one time. The total number of available seat licenses in the pool is determined by the Edge model you have and any upgrade licenses you apply.

The main Firebox Users page (under **Active Sessions**) shows how many seat licenses are in use when you require users to authenticate before accessing resources. This page also shows the maximum number of seat licenses currently allowed.

A seat license is used when the Edge allows traffic to be passed from a computer on the trusted or optional network to the external network (typically the Internet). Forcing users to authenticate before accessing the external network ensures that no seat licenses are used by machines that are not authorized to access the external network. If a user or computer tries to access the external network without authenticating, and authentication is required, the Edge does not

allow the traffic to pass. A seat license is consumed only when traffic is allowed to pass from behind the Edge to the external network.
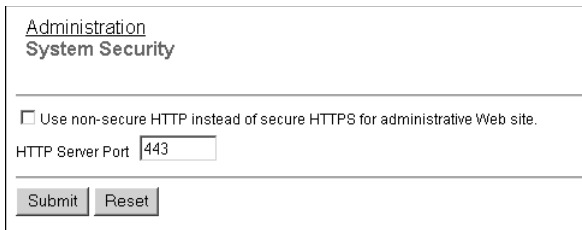
Selecting HTTP or HTTPS for Firebox Management

HTTP (Hypertext Transfer Protocol) is the "language" used for transferring files (text, graphic images, and multimedia files) on the Internet. HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) is similar except that it enhances computer security by encrypting and decrypting the names of Web pages you type into your browser. For greater security, the Firebox® X Edge uses HTTPS by default.

Follow these instructions to use the less secure HTTP instead of HTTPS:

1   Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox.
    The default IP address is: https://192.168.111.1

2   From the navigation bar, select
    Administration > **System Security**.
    The System Security page appears.

3   Select the **Use non-secure HTTP instead of secure HTTPS for administrative Web site** checkbox.

4   Click **Submit**.

If you select this checkbox, you must use http:// in the browser's address bar to bring up configuration pages instead of the default https://.

Changing the HTTP Server Port

To connect to the Firebox X Edge to view its configuration pages, or for a user to authenticate to the Edge, the browser's connection must use the same port as the Edge's HTTP server port. Because HTTPS uses TCP port 443 (HTTP uses TCP port 80), the default HTTP server port for the Edge is 443.

To change the port over which you communicate with the Firebox X Edge, type a new value in the **HTTP Server Port** field, as shown in the previous figure.

Setting up VPN Manager Access

Use the VPN Manager Access page to allow your Firebox X Edge to be remotely managed by WatchGuard VPN Manager.

VPN Manager does not run directly on your Firebox X Edge; it is separate software that runs on a WatchGuard Firebox III or Firebox X. It configures and manages VPN tunnels.

For more information about VPN Manager, see the WatchGuard Web site:

https://www.watchguard.com/products/vpnmanager.asp

Follow these instructions to configure VPN Manager access:

1   Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
    The default IP address is: https://192.168.111.1

2   From the navigation bar, select
    Administration >**VPN Manager Access**.
    The VPN Manager Access page appears.

```
Administration
VPN Manager Access


☑ Enable VPN Manager Access
              Status Passphrase  [**********]
      Confirm Status Passphrase  [**********]
       Configuration Passphrase  [**********]
Confirm Configuration Passphrase  [**********]
☑ Compatible with pre WFS 7.3 VPN Manager

[ Submit ]  [ Reset ]
```

3   Select the **Enable VPN Manager Access** checkbox.

4   Type the status passphrase and then type it again to confirm in
    the applicable fields.

5   Type the configuration passphrase and then type it again to
    confirm in the applicable fields.

─────────────────────── **NOTE** ───────────────────────
These passphrases must match the passphrases used in the VPN
Manager software or the connection will fail.

6   Select the **Compatible with pre WFS 7.3 VPN Manager** button
    if you want to use WatchGuard System Manager 7.0, 7.1, or 7.2
    to manage your Edge.

7   Click **Submit**.

Updating the Firmware

Check regularly for Firebox® X Edge updates on the WatchGuard
Web site:

   https://www.watchguard.com/support/sohoresources

Two different methods exist for updating the firmware. One method
uses a slightly larger download and automatically updates the firm-
ware on the Firebox X Edge when run from any computer running
Windows. The other method uses a smaller download and allows

you to update the firmware through the Firebox X Edge Web pages. If you configure your Firebox X Edge from a computer that does not use the Windows operating system, such as Macintosh or Linux, you must update your firmware with the second procedure because those operating systems cannot run Windows executable files.

Method 1

The first method uses an auto-executable file and is the preferred method for updating the Firebox X Edge firmware from a Windows computer. Download the Software Update Installer to use this method. To use the Software Update Installer:

1 Launch the installer on a computer running Windows that is on the trusted side of the Firebox X Edge.

2 The installer prompts for an IP address and a user name and password. Enter the Firebox X Edge's trusted interface IP address.
   By default this is 192.168.111.1

3 Enter the administrator name and password. Click **OK**.
   The installer updates the firmware on the Firebox X Edge. As part of the update process, the Firebox X Edge will reboot once or twice— this is normal.

4 When the **Finish** button appears, click it.

─────────────── **NOTE** ───────────────
Because the Installer uses FTP to transfer files, make sure your Firebox X Edge is not configured to deny FTP access, as described in "Denying FTP access to the trusted network interface" on page 86.
──

Method 2

The second method uses the Firebox X Edge Web pages. You can use this method regardless of the operating system your computer is running. You must first download the Software Update file, a small Zip file.

1 Extract the "wgrd" file from the Zip file you downloaded using an archiving utility such as Winzip (for Windows computers), Stuffit (for Macintosh), or Linux's archive capabilities.

2   Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1

3   From the navigation bar, select
Administration > Update.
The Administration Page appears with the End User License Agreement (EULA).

4   Read the text of the EULA. If you agree, select the **I accept the above license agreement** checkbox.

5   Type the name of the file containing the new Firebox X Edge software in the **Select file** box. Or click **Browse** to locate the file on the network.

6   Click **Update** and follow the instructions.

Activating Upgrade Options

Every Firebox® X Edge includes the software for all upgrade options, although they are not available for your use until you enter a license key for them in the configuration of the Firebox. To receive a license key, purchase and activate an upgrade option at the LiveSecurity Service Web site or from a WatchGuard-authorized reseller. See "Registering Your Edge and Activating LiveSecurity Service" on page 26 for more information.

After you have purchased an upgrade option, follow these steps to activate it:

1   Go to the upgrade page of the WatchGuard Web site:
http://www.watchguard.com/upgrade

2   Type your LiveSecurity Service user name and password in the fields provided.

3   Click **Log In**.

4   Follow the instructions provided on the Web site to activate your license key and to retrieve the feature key.

5   Copy the feature key from the LiveSecurity Service Web site.
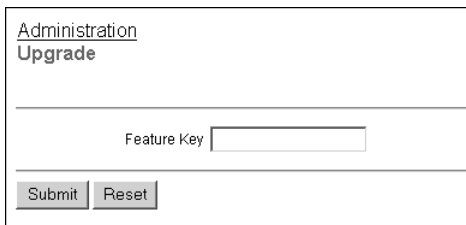
6   Type the IP address of the trusted network in your browser
     window to connect to the System Status page of the Firebox X
     Edge.
     The default IP address is: https://192.168.111.1

7   From the navigation bar, select
     Administration >**Upgrade**.
     The Upgrade page appears.

```
Administration
Upgrade
_____

            Feature Key [                    ]

 [ Submit ]  [ Reset ]
```

8   Paste the feature key in the applicable field.

9   Click **Submit**.

Upgrade options

User licenses

A seat license upgrade allows more connections between the
trusted network and the external network. For example, a 10-
seat license allows 10 connections instead of the standard five
connections.

MUVPN Clients

The MUVPN Clients upgrade allows remote users to connect to
the Firebox X Edge through a secure (IPSec) VPN tunnel. These
users have access to trusted network resources.

WebBlocker

The WebBlocker upgrade enables the Web filtering option. For
more information on WebBlocker, see the "Configuring
WebBlocker" chapter.

Enabling the Model Upgrade Option

A model upgrade gives you the same capability you would get if you
purchased the higher model. For example, an upgrade from Firebox
X5 to X50 is like getting a new Firebox X50 right off the shelf. A
model upgrade provides increased speed, greater capacity, more user

licenses, more concurrent sessions, and more VPN tunnels. For a datasheet showing the capabilities of the different Firebox X Edge models, go to:

http://www.watchguard.com/docs/datasheet/edge_ds.asp

You can upgrade an X5 or an X15 to any higher model.

1   Go to the Activation Center on the WatchGuard Web site (www.watchguard.com/upgrade) and log into your LiveSecurity Service account.

2   In the space provided, enter the license key exactly the way it appears on your printed certificate or your online store receipt, including any hyphens. Click **Continue** and follow the instructions.

Configuring Additional Options

Other options for your Firebox® X Edge do not require that you purchase them separately. However, they are initially disabled on your Firebox, and you must configure them. These options are as follows:

Managed VPN
The managed VPN feature allows you to set up VPN tunnels using DVCP. For more information, see Chapter 8, "Configuring VPNs."

Manual VPN
The manual VPN feature allows you to set up VPN tunnels manually. For more information, see Chapter 8, "Configuring VPNs."

WAN Failover
The WAN failover feature adds redundant support for the external interface. For more information, see "Enabling the WAN Failover Option" on page 64.

Viewing the Configuration File

You can view the contents of the Firebox® X Edge configuration file in text format from the View Configuration page.

1   Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
    The default IP address is: https://192.168.111.1

2   From the navigation bar on the left side, select **Administration** >**View Configuration File**.

```
Administration
View Configuration File


FDATE: Jun  4 2004
FTIME: 09:19:22
FVER: 7.0.0
admin.external_access: 1
admin.ha1hash: e80721f9ad6f03b50e89c8a08d082dc3
admin.idle_timeout: 0
admin.ipsec_access: 1
admin.max_access: 0
admin.muvpn_access: 0
admin.name: admin
admin.pass: pass
config.version: 0.1
networking.dhcp_client.enable: 0
networking.dhcpd.enable: 0
networking.dhcpd.firstip: 192.168.111.2
networking.dhcpd.lastip: 192.168.111.252
networking.dhcpd.optional.enable: 0
networking.dhcpd.optional.firstip: 192.168.112.2
networking.dhcpd.optional.lastip: 192.168.112.252
networking.ethernet.00: eth0 192.168.54.54 192.168.54.0 255.255.255.0 192.168.54.254
networking.ethernet.00.linkspeed: 1
networking.ethernet.01: eth1 192.168.111.1 192.168.111.0 255.255.255.0 192.168.111.1
networking.ethernet.02: eth2 192.168.112.1 192.168.112.0 255.255.255.0 192.168.112.1
networking.nameservice.dhcpd.dns.0: 192.168.130.131
networking.nameservice.dhcpd.dns.1: 192.168.130.245
networking.nameservice.dhcpd.domain_suffix: wgti.net
```

Firebox® X Edge Hardware

The WatchGuard® Firebox® X Edge is a firewall for small organizations and branch offices. The WatchGuard Firebox X Edge wireless has a built-in access point for connecting computers with wireless capability.

Package Contents

The Firebox® X Edge package also has:

- The Firebox X Edge *User Guide*
- The Firebox X Edge *QuickStart Guide*
- A LiveSecurity® Service activation card

- A Hardware Warranty Card

- An AC adapter (12 V)

- Power cable clip, to attach to the cable and connect to the side of the Edge. This releases tension on the power cable.

- One straight-through cable

FIREBOX® X EDGE PACKAGE CONTENTS:

QuickStart Guide

Upgrade Key (X50 MODELS ONLY)

LiveSecurity® Activation Card

Edge

User Guide

AC Adapter

Straight Through Ethernet Cable
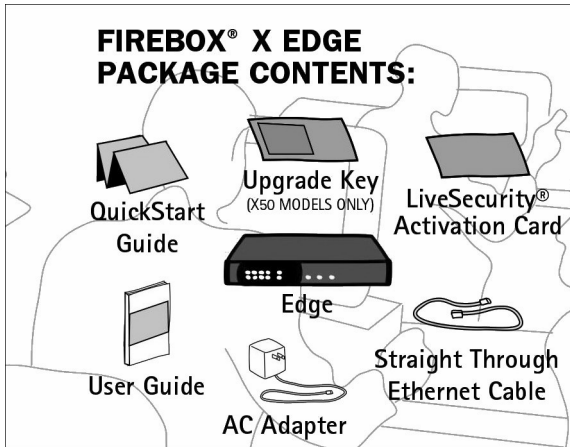
Specifications

Processor	64 bit MIPS
Memory - Flash	16 MB
Memory - RAM	64 MB
Ethernet interfaces	10 each 10/100
Serial ports	1 DB9
Power supply	12V DC
Operating Temperature	0 - 40C
Dimensions	Depth = 5.75 inches Width = 8.75 inches Height = 1.25 inches
Weight	1.9 U.S. pounds

Hardware Description

The Firebox X Edge has a simple hardware architecture. All indicator lights appear on the front panel while all ports and connectors are on the rear of the device.

Front panel

The front panel of the Firebox X Edge has 24 indicator lights to show the link status. The top indicator light in each link pair comes on when a link is established and flashes when traffic goes through the related interface. The bottom indicator light in each pair comes on when the link speed is 100 Mbps. If the bottom indicator light does not come on, the link speed is 10 Mbps.
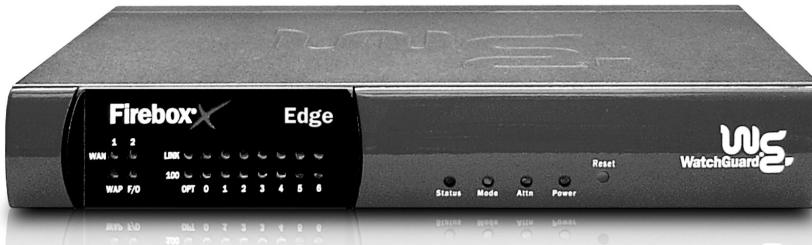
WAN 1, 2

Shows a physical connection to the external Ethernet interfaces. The indicator light is yellow when traffic goes through the related interface.

WAP

Shows a wireless connection to the Edge. The indicator light is green when traffic goes through the wireless interface on a Firebox X Edge Wireless model.

F/O

Shows a WAN failover. The indicator light is green when there is a WAN failover from WAN1 to WAN2. The indicator light goes off when the external interface connection goes back to WAN1.

Link

The link indicator light shows a physical connection to a trusted Ethernet interface. The trusted interfaces have the numbers 0 through 6. The indicator light comes on when traffic goes through the related interface.

100

When a trusted network interface operates at 100 Mbps, the related 100 indicator light comes on. When it operates at 10 Mbps, the indicator light does not come on.

Status

Shows a management connection to the Edge. The indicator light goes on when you use your browser to connect to the Edge configuration pages. The indicator light goes off a short time after you close your browser.

Mode

Shows the status of the external network connection. The indicator light comes on when the Ethernet cable is correctly connected to the WAN1 interface. The indicator light is green if the Edge can connect to the external network and send traffic. The indicator light flashes if the Edge cannot connect to the external network and send traffic.

Attn

Reserved for future use.

Power

Shows that the Firebox X Edge is on.

RESET button

Push the RESET button to set the Firebox X Edge to the factory default configuration. For more information, see "Factory Default Settings" on page 41.

Back view
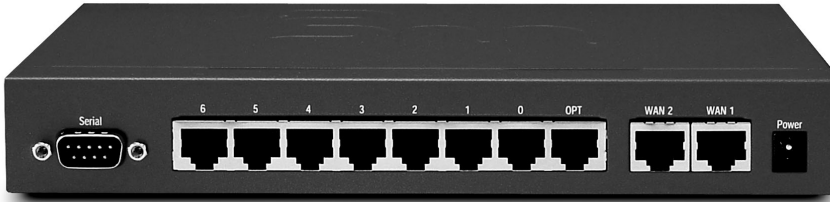
Serial port (DB9)

Use the serial port to connect an external modem to the Edge.

Ethernet interfaces 0 through 6

The 7 Ethernet interfaces with the marks 0 through 6 are for the trusted network.

OPT interface

This Ethernet interface is for the optional network.

WAN interfaces 1 and 2

The WAN1 and WAN2 interfaces are for the external network.

Power input

We supply a 12-volt AC adaptor with your Edge. Connect the AC adapter to the Edge and to a power source. The power supply tip is plus (+) polarity.

Side panels

Computer Lock Slot

There is a slot for a computer lock on the two side panels of the Firebox X Edge.

Antennae (wireless model only)

There are wireless antennae on the two side panels of the Firebox X Edge wireless models.

Index

D

daylight savings time 95
default factory settings 41—42
Denied Sites page 104
DHCP
    described 5, 47
    setting the Firebox to use 23
    setting your computer to use 20
DHCP address reservations
    setting on the optional network 58
    setting on the trusted network 53
DHCP Address Reservations page 53, 58
DHCP relay
    configuring the optional network 58
    configuring the trusted network 53
DHCP relay agent, configuring Firebox
    as 54
DHCP relay agent, configuring the
    optional network as 59
DHCP server
    configuring Firebox as 51, 56
dialog boxes
    Internet Protocol (TCP/IP) Properties
        21
Dial-Up Networking, installing 123
Diffie-Hellman groups 115
Digital Subscriber Line (DSL) 2
DNS service, dynamic 62
DNS, described 6
Domain Name Service
    described 6
DSL 3
DVCP, described 111
Dynamic DNS client page 63
dynamic DNS service, registering with
    62—63
Dynamic Host Configuration Protocol.
    See DHCP
Dynamic VPN Configuration Protocol,
    described 111

E

echo host 118
Enable PPPoE debug trace checkbox 26,
    49
encrypted connections on optional
    network 60
event, described 91
external interface
    configuring 23—26
external network
    described 9
    if ISP uses DHCP 47
    if ISP uses PPPoE 48
    if ISP uses static addressing 48
External Network Configuration page
    25

F

factory default settings
    described 41
    resetting to 42
failover network. See WAN failover
feature key
    described 26
File and Printer Sharing for Microsoft
    Networks
    and Windows XP 129
File and Printer Sharing for Microsoft
    Networks, installing 127
Filter Traffic page 80, 83
Firebox Users page 34, 152, 155
Firebox X Edge
    administrator account 154
    cabling 17
    configuring as DHCP server 51
    described 165
    front panel 167
    hardware description 167—169
    hardware specifications 167
    indicator lights 167
    installing 11—27
    package contents 12, 165
    rebooting 42—44

W

Z